COEG-09-20

Acuerdo de la Comisión de Organización Electoral y Geoestadística, por el que se aprueba la designación del ente auditor del Sistema Electrónico por Internet del Instituto Electoral de la Ciudad de México para la Elección de las Comisiones de Participación Comunitaria 2020 y la Consulta de Presupuesto Participativo 2020 y 2021

A n t e c e d e n t e s:

I. El 10 de febrero de 2014, se publicó en el Diario Oficial de la Federación, el Decreto por el que se reforman, adicional y derogan diversas disposiciones de la Constitución Política de los Estados Unidos Mexicanos, en materia política – electoral. (Constitución Federal).

II. El 5 de febrero de 2017, se publicó en la Gaceta Oficial de la Ciudad de México (Gaceta Oficial) el Decreto por el que se expidió la Constitución Política de la Ciudad de México (Constitución Local).

III. El 7 de junio de 2017, se publicó en la Gaceta Oficial el Decreto por el cual se abrogó, entre otros, el Código de Instituciones y Procedimientos Electorales del Distrito Federal y la Ley Procesal Electoral del Distrito Federal y se expidió el Código de Instituciones y Procedimientos Electorales de la Ciudad de México (Código) y la Ley Procesal Electoral para la Ciudad de México (Ley Procesal).

IV. El 4 de agosto de 2017, el Consejo General del Instituto Electoral de la Ciudad de México (Consejo General), aprobó el Reglamento Interior del Instituto Electoral de la Ciudad de México (Reglamento Interior), mediante Acuerdo IECM/ACU-CG-016/2017.

V. El 31 de enero de 2019, el Consejo General aprobó mediante Acuerdo IECM/ACU-CG-008/2019 la creación del Comité Técnico que emitirá la

opinión sobre el estado actual del Sistema Electrónico por Internet y, en su caso, la recomendación de su utilización en la Elección de Comités Ciudadanos y Consejos de los Pueblos 2019 y en la Consulta Ciudadana sobre Presupuesto Participativo 2020.

VI. El 12 de marzo 2019, el Comité Técnico del SEI presentó y aprobó el documento "Opinión del Comité Técnico sobre el estado actual del Sistema Electrónico por Internet y recomendación de su utilización en la Elección de Comités Ciudadanos y Consejos de los Pueblos 2019 y Consulta Ciudadana sobre Presupuesto Participativo 2020.

VII. El 12 de agosto de 2019, se publicó en la Gaceta Oficial, el Decreto por el que se abroga la Ley de Participación Ciudadana del Distrito Federal y se expide la Ley de Participación Ciudadana de la Ciudad de México (Ley de Participación), entrando en vigor al momento de su publicación.

VIII. Derivado de lo anterior el 29 de octubre de 2019, la Comisión de Organización Electoral y Geoestadística (COEG):

- Aprobó el *"Estudio de Viabilidad Técnica, Operativa y Financiera que presentan la Dirección Ejecutiva de Organización Electoral y Geoestadística y la Unidad Técnica de Servicios Informáticos para proponer el uso del Sistema Electrónico por Internet, como una modalidad adicional para recabar los votos y opiniones de la Ciudad de México en la Elección de Comisiones de Participación Comunitaria 2020 y la Consulta en Materia de Presupuesto Participativo 2020 y 2021"* (Acuerdo COEG/47/2019).

- Aprobó la "*Guía para la implementación del Sistema Electrónico por Internet en la Elección de Comisiones de Participación Comunitarias 2020*

y la Consulta en Materia de Presupuesto Participativo 2020 y 2021". (Acuerdo COEG/48/2019).

- Aprobó e instruyó presentar ante el Consejo General el *Proyecto de Acuerdo del Consejo General del Instituto Electoral, por el que se aprueba el uso del Sistema Electrónico por Internet como una modalidad adicional para recabar votos y opiniones en la Elección de Comisiones de Participación Comunitaria 2020 y la Consulta en Materia de Presupuesto Participativo 2020 y 2021.* (Acuerdo COEG/49/2019).

IX. El 16 de noviembre de 2019, el Consejo General de este Instituto Electoral:

- Mediante Acuerdo IECM/ACU-CG-077/2019 aprobó *"Los Lineamientos Generales del Sistema Electrónico por Internet del Instituto Electoral de la Ciudad de México"* (Lineamientos del SEI).

- Mediante Acuerdo IECM/ACU-CG-078/2019 aprobó *el uso del Sistema Electrónico por Internet, como una modalidad adicional para recabar los votos y las opiniones en la Elección de Comisiones de Participación Comunitaria 2020 y la Consulta de Presupuesto Participativo 2020 y 2021.*

- Mediante Acuerdo IECM/ACU-CG-079/2019, aprobó la *"Convocatoria Única para la Elección de Comisiones de Participación Comunitaria 2020 y la Consulta de Presupuesto Participativo 2020 y 2021".*

X. El 4 de febrero de 2020, mediante Oficio IECM/UTSI/036/2020 se envió a siete instituciones académicas la invitación para participar en el Proceso de Selección de Auditores Externos del SEI para la Elección de las Comisiones de Participación Comunitaria 2020 y la Consulta de Presupuesto Participativo 2020 y 2021 (Elección 2020 y Consulta 2020 y 2021), las cuales se anexan al presente documento:

- Centro de Investigación en Computación del Instituto Politécnico Nacional (CIC-IPN).
- Centro Tecnológico Aragón de la Facultad de Estudios Superiores Aragón (UNAM).
- Centro de Investigación y Docencia Económicas.
- Dirección General de Cómputo y Tecnologías de Información y Comunicaciones de la Universidad Nacional Autónoma de México.
- Colegio de México.
- Escuela Superior de Ingeniería Mecánica y Eléctrica Unidad Culhuacán del Instituto Politécnico Nacional.
- Universidad Autónoma Metropolitana.

Considerandos:

1. Que, de conformidad con lo dispuesto en el artículo 41, párrafo segundo, Base V, Apartado C, numeral 9 de la Constitución Federal, el Instituto Electoral tiene dentro de sus funciones la organización, desarrollo, cómputo y declaración de resultados en los mecanismos de participación ciudadana conforme lo prevea la legislación local.

2.Que, de acuerdo con el artículo 25, apartado A, numeral 2 de la Constitución Local; y el diverso 6, fracción I del Código, las autoridades de la Ciudad garantizarán la democracia participativa, entendida como el derecho de las personas a incidir, individual y colectivamente, en las decisiones públicas y en la formulación, ejecución, evaluación y control del ejercicio de la función pública, en los términos que las leyes señalen y que son derechos de las y los ciudadanos de la Ciudad de México, votar y participar en los Procesos Electorales así como en los mecanismos e instrumentos de Participación Ciudadana conforme lo dispuesto al propio Código y demás disposiciones aplicables.

3. Que, según lo previsto en los artículos 37, fracciones I, III, V y VI y 98 fracción II del Código, el Instituto Electoral cuenta entre otros órganos, con un Consejo General; una Secretaría Ejecutiva, Direcciones Ejecutivas, entre las cuales se encuentra la Dirección Ejecutiva de Organización Electoral y Geoestadística (DEOEyG), así como diversos Órganos Técnicos, entre los cuales se encuentra la Unidad Técnica de Servicios Informáticos (UTSI).

4. Que, en cumplimiento a lo previsto por los artículos 52 y 58 del Código, el Consejo General cuenta con el auxilio de Comisiones Permanentes y Comités para el desempeño de sus atribuciones, cumplimiento de obligaciones y supervisión del adecuado desarrollo de las actividades de los órganos ejecutivos y técnicos del Instituto Electoral, así como vigilar la ejecución de los programas institucionales y la realización de tareas específicas que haya determinado el propio Órgano Superior de Dirección.

5. Que, conforme a los artículos 8 y 14, el Instituto Electoral es autoridad en materia de democracia directa y participativa, la cual debe asegurar que los mecanismos e instrumentos, en sus modalidades presencial y digital, sigan parámetros internacionales de accesibilidad con el objeto de garantizar la participación de todas las personas.

6. Que, el artículo 29, fracciones IX y XII del Reglamento Interior del Instituto Electoral de la Ciudad de México, la UTSI tiene entre sus atribuciones, investigar y analizar permanentemente el uso de nuevas tecnologías en materia de informática y telecomunicaciones para proponer su aplicación, así como desarrollar sistemas informáticos en material electoral y administrativa como una herramienta que apoye el cumplimiento de los fines institucionales.

7. Que, las nuevas tecnologías de la información, aplicadas a los procesos electorales y de participación ciudadana, permiten su utilización, principalmente, en dos modalidades:

a) Votación Presencial: Requiere que la ciudadanía acuda a un lugar determinado por la autoridad electoral, en el cual se instalan dispositivos electrónicos para la emisión del voto;

b) Votación a Distancia Remota: Consiste en el uso de aplicaciones informáticas que funcionan sobre una plataforma en Internet para la emisión de los votos por parte de la ciudadanía.

Esta segunda modalidad constituye una herramienta útil y económica para fortalecer la participación en diversos ejercicios de votación, misma que, a partir de su regulación electoral en la Ciudad de México, ha sido impulsada por el Instituto Electoral para potenciar el ejercicio del derecho al voto entre la ciudadanía.

8. Que, la Sala Superior del Tribunal Electoral del Poder Judicial de la Federación, a través de la sentencia en el expediente del Juicio de Revisión Constitucional Electoral SUP-JRC-306/2011, consideró al SEI como un sistema con estándares suficientes de seguridad y niveles razonables de confianza, dada su idoneidad para garantizar la emisión del voto, de acuerdo con los principios universalidad, libertad, secrecía, en cuyo caso, las claves de acceso al sistema, así como a la boleta virtual son personales.

9. Que, la implementación del SEI en los procesos de participación ciudadana atiende a medidas razonables de seguridad y permite solventar situaciones diversas a las que la ciudadanía se pueda enfrentar para ejercer su derecho a emitir su voto y opinión.

10. Que, conforme a lo establecido en el artículo 1 de los Lineamientos del SEI, dicho documento tiene como finalidad regular el desarrollo de dicho Sistema, así como establecer y describir las fases que rigen los componentes y operaciones asociados al Sistema, debiendo cumplirse cada una de ellas.

11. Que, el artículo 8 inciso e) de los Lineamientos del SEI, establece que la Secretaría Ejecutiva a través de la UTSI apoyará con la instrumentación y operación del SEI.

12. Que, los artículos 47 y 48 de los Lineamientos del SEI señalan que previo a la operación del Sistema, se deberán realizar las pruebas de funcionalidad, capacidad, continuidad y seguridad a las herramientas informáticas que se estimen pertinentes y, al menos, dos simulacros que incluyan la ejecución de todas las fases del Sistema, por lo que el Instituto Electoral podrá someterlo a una auditoría pública en cada una de sus etapas de desarrollo e implementación, a través de instituciones o empresas con prestigio internacional. Lo anterior se hará en acompañamiento de partidos políticos, candidaturas sin partido y, en su caso, observadores de la Sociedad Civil.

13. Que, de acuerdo con lo estipulado en el artículo 49 de los Lineamientos del SEI, la Auditoría tendrá la finalidad de evaluar la funcionalidad y seguridad en el procesamiento de la información y cubrirá, como mínimo, los siguientes puntos:

I.- Planificación de la auditoría, identificando claramente su alcance, así como los recursos materiales y técnicos necesarios para llevarla a cabo;

II.- Metodología de la auditoría, incluyendo procedimientos, plazos y enfoque para verificar y comprobar los controles a revisar, así como formato y contenido de reportes que se deriven de ésta;

III. La revisión del Sistema, aplicando pruebas de aseguramiento de calidad y pruebas de seguridad.

Las pruebas de aseguramiento de calidad deberán estar conformadas por al menos los siguientes tipos de prueba:

a) Pruebas de funcionalidad, para verificar que el Sistema hace exclusivamente lo que debe hacer, conforme a la especificación técnica, y

b) Pruebas de desempeño, para evaluar la respuesta del Sistema bajo condiciones en donde se simule un alto número de solicitudes simultáneas.

Las pruebas de seguridad deberán estar conformadas por al menos los siguientes tipos de prueba:

- Análisis de vulnerabilidades, al Sistema e infraestructura tecnológica que éste utilice de manera central;
- Pruebas de denegación de servicio, para verificar la respuesta del Sistema y la infraestructura tecnológica bajo un escenario simulado de ataque informático;
- Pruebas de penetración, para verificar la correcta resistencia ante posibles ataques que intenten modificar la funcionalidad del Sistema;
- Pruebas de estrés basadas en la funcionalidad del Sistema bajo cargas con un gran número de repeticiones, manejo de grandes cantidades de datos y un alto número de consultas a la base de datos, con la finalidad de que el Sistema brinde una operación por encima de la media esperada para verificar su desempeño.

IV. Revisión del manejo seguro de la información; y

V. En su caso, la revisión de los sistemas informáticos que el Instituto así defina.

14. Que, tal y como se menciona en el artículo 50 de los Lineamientos del SEI, se deberá elaborar un instrumento jurídico que deberá como mínimo establecer los siguientes elementos:

I. Los alcances mínimos de la auditoría, establecidos en los presentes Lineamientos y el plan de trabajo asociado al mismo;

II. La información que la autoridad electoral administrativa pondrá a disposición del ente auditor, salvaguardando en todo momento los derechos de la propiedad intelectual y la protección de los datos personales de las y los ciudadanos; y

III. Las responsabilidades de las partes para la realización de la auditoría.

15. Que, el artículo 52 establece que el ente auditor deberá presentar informes parciales y un dictamen final del proceso de auditoría debiendo considerar lo siguiente:

I. Informes parciales: son los referentes a los resultados emitidos durante el proceso de auditoría. Deberán incluir, al menos lo siguiente:

a) Los criterios utilizados para la revisión;

b) El método para clasificar los hallazgos que permitan priorizar su atención;

c) Los hallazgos identificados y clasificados, y

d) Las posibles recomendaciones que permitan al Instituto Electoral atenderlos.

II. Dictamen: Documento público con el resultado final de la auditoría que contendrá de manera enunciativa, más no limitativa, que el Sistema permite lo siguiente:

a) El acceso se otorgue exclusivamente a las personas ciudadanas registradas para emitir su sufragio por Internet;

b) Que la o el ciudadano emita solamente un sufragio por elección mediante este mecanismo;

c) Que se preserve la secrecía del sufragio; y

d) La efectiva emisión, transmisión, recepción y cómputo del sufragio emitido.

16. Que, en respuesta al Oficio IECM/UTSI/036/2020, relacionado en el antecedente décimo, el 6 de febrero de 2020 se recibió mediante Oficio FESAR/CTA/025/2020, la Propuesta Técnico – Económica para la auditoría al SEI, así como su síntesis curricular en materia de auditorías, por parte del "Centro Tecnológico Aragón" de la Facultad de Estudios Superiores Aragón (Fes Aragón), documentos que se anexan al presente.

17. Que, con la misma fecha, la Universidad Nacional Autónoma de México (UNAM) mediante Oficio TIC/DCV/005/2020, informó que no está en condiciones de presentar la propuesta solicitada debido a compromisos previamente establecidos y en virtud de que la invitación se extendió a toda la Dirección General de Cómputo y de Tecnologías de Información y Comunicación (DGTIC), consideran oportuno manifestar que en el supuesto de que la UNAM decidiera presentar la propuesta solicitada, lo realizaría a través de la Facultad de Estudios Superiores Aragón, quien de igual forma, recibió una invitación similar, documento que se anexa al presente.

18. Que, el 7 de febrero de 2020, mediante Oficio CIC/0308/20, el Centro de Investigación en Computación del Instituto Politécnico Nacional (CIC-IPN), informó que encuentra inviables los periodos definidos para la presentación de una propuesta técnica que permita cumplir en tiempo y forma con los servicios que este Instituto Electoral requiere, documento que se anexa al presente.

19. Que, conforme a la Evaluación Técnica que realizó la UTSI el día 10 de febrero de 2020, se determinó que la Fes Aragón **CUMPLE** en su totalidad con las

especificaciones solicitadas, la cual se anexa como parte integral del presente Acuerdo.

20. Que, por parte de las siguientes instituciones académicas no se tuvo respuesta a la invitación para participar como Ente Auditor del SEI:

- Centro de Investigación y Docencia Económicas.
- Colegio de México.
- Escuela Superior de Ingeniería Mecánica y Eléctrica Unidad Culhuacán del Instituto Politécnico Nacional.
- Universidad Autónoma Metropolitana.

En razón de lo expuesto y fundado, se emite el siguiente:

A c u e r d o

PRIMERO. Se aprueba la designación del "Centro Tecnológico Aragón" de la Facultad de Estudios Superiores Aragón, como ente auditor del Sistema Electrónico por Internet del Instituto Electoral de la Ciudad de México para la Elección de las Comisiones de Participación Comunitaria 2020 y la Consulta de Presupuesto Participativo 2020 y 2021.

SEGUNDO. Se instruye al Secretario Ejecutivo para que, en el ámbito de sus atribuciones, instruya a las áreas técnicas del Instituto Electoral para la elaboración del instrumento jurídico, en términos del considerando décimo cuarto del presente Acuerdo.

Así lo aprobaron por unanimidad de votos las consejeras electorales integrantes de la Comisión Permanente de Organización Electoral y Geoestadística, en la tercera sesión extraordinaria del 17 de febrero de 2020, quienes firman al calce.

Myriam Alarcón Reyes
Consejera Electoral presidenta de la Comisión

Carolina del Angel Cruz
Consejera Electoral integrante de la Comisión

Gabriela Williams Salazar
Consejera Electoral integrante de la Comisión

INSTITUTO ELECTORAL CIUDAD DE MÉXICO

ACUSE

UNIDAD TÉCNICA DE SERVICIOS INFORMÁTICOS

Ciudad de México, a 4 de febrero de 2020
IECM/UTSI/036/2020

Dr. Marco Antonio Ramírez Salinas
Director del Centro de Investigación en Computación del
Instituto Politécnico Nacional (CIC-IPN)
Av. Juan de Dios Batiz, Esq. Miguel Othón de Mendizábal
Col. Nueva Industrial Vallejo, Gustavo A. Madero
C.P. 07738 Ciudad de México

INSTITUTO POLITÉCNICO NACIONAL
CIC-DIRECCIÓN
CONTROL DE GESTIÓN
RECIBIÓ: 04 FEB 2020
HORA: 12:12

PRESENTE

El Instituto Electoral de la Ciudad de México (Instituto Electoral) comprometido con la ciudadanía de la entidad y con potenciar el ejercicio de sus derechos políticos-electorales, ha realizado permanentemente trabajos de investigación tendentes a conocer y analizar las diversas tecnologías que permitan la modernización, automatización y reducción de costos, de los procesos electorales y de participación ciudadana, específicamente para la recepción y cómputo de votos y opiniones.

Como parte de las actividades institucionales de este año, el Instituto Electoral realizará la Elección de Comisiones de Participación Comunitaria 2020 y la Consulta de Presupuesto Participativo 2020 y 2021 en la cuales, se utilizará el Sistema Electrónico por Internet (SEI) como un mecanismo adicional para recabar los votos y las opiniones de dichos ejercicios; por tal motivo y con la intención de incrementar el nivel de confianza en la ciudadanía, este Instituto tiene considerado llevar a cabo una auditoría informática al citado sistema.

Considerando que el 28 de octubre de 2019, este Instituto Electoral aprobó el Estudio de viabilidad técnica, operativa y financiera para proponer el uso del Sistema Electrónico por Internet para recabar los votos en las demarcaciones Cuauhtémoc y Miguel Hidalgo de forma presencial y remota

En tal virtud, se extiende una cordial invitación para que participe en el proceso de selección de Auditores Externos para la Elección 2019 y en la Consulta Ciudadana 2020. En el caso de que sea de su interés le solicito de la manera más atenta y de no existir inconveniente; se envíe por escrito y de forma electrónica a la dirección utsi@iecm.mx su propuesta Técnico-Económica a más a tardar el 7 de febrero del presente año

INSTITUTO ELECTORAL CIUDAD DE MÉXICO

UNIDAD TÉCNICA DE SERVICIOS INFORMÁTICOS

Ciudad de México, a 4 de febrero de 2020
IECM/UTSI/036/2020

Lo anterior para dar continuidad a la invitación realizada mediante oficio IECM/UTSI/082/2019 para participar como Auditor Externo; así como su respuesta a través de oficio No CIC/0610/2019 en el que manifiesta el interés en participar (anexo copia de los oficios citados)

A efecto de tener los elementos necesarios para elaborar la propuesta referida, me permito indicar las ligas de Internet, donde se podrán consultar la convocatoria y la guía de implementación del Sistema Electrónico por Internet. Así mismo anexo los requerimientos que se deberán atender para la Auditoría de mérito.

- https://www.iecm.mx/www/taip/cg/acu/2019/IECM-ACU-CG-079-2019.pdf
- https://www.iecm.mx/www/taip/cg/acu/2019/IECM-ACU-CG-078-2019.pdf

Sin otro particular, reciba un cordial saludo

ATENTAMENTE

Lic. Oscar Alejandro Rodríguez Paz
Titular de Unidad Técnica de Servicios Informáticos

C.P. **Mtro. Mario Velázquez Miranda**, Consejero Presidente del Instituto Electoral de la Ciudad de México. Presente
Mtra. Myriam Alarcón Reyes, Presidenta de la Comisión de Organización Electoral y Geoestadística del Instituto Electoral de la Ciudad de México. Presente
Mtra. Carolina del Angel Cruz, Integrante de la Comisión de Organización Electoral y Geoestadística del Instituto Electoral de la Ciudad de México. Presente
Mtra. Gabriela Williams Salazar, Integrante de la Comisión de Organización Electoral y Geoestadística del Instituto Electoral de la Ciudad de México. Presente
Lic. **Rubén Geraldo Venegas**, Secretario Ejecutivo del Instituto Electoral de la Ciudad de México. **Presente**
Mtro. **Alejandro Fidencio González Hernández**, Secretario Administrativo del Instituto Electoral de la Ciudad de México. Presente
Lic. Cecilia A. Hernández Cruz, Titular de la Unidad Técnica de Vinculación con Organismos Externos del Instituto Electoral de la Ciudad de México. Presente
Archivo

OARP/NFP.Emi.

Sistema de Gestión de Calidad

Certificado

Huizaches No. 25, Colonia Rancho Los Colorines, Tlalpan, C.P. 14386, Ciudad de México. Conmutador 5483-3800

INSTITUTO ELECTORAL CIUDAD DE MÉXICO

ACUSE

UNIDAD TÉCNICA DE SERVICIOS INFORMÁTICOS

Ciudad de México, a 4 de febrero de 2020
IECM/UTSI/036/2020

Dr. Jacinto Cortés Pérez
Coordinador del Centro Tecnológico Aragón de la
Facultad de Estudios Superiores Aragón (UNAM)
Av. Rancho Seco S/N Col. Impulsora
C.P. 51170 Cd. Nezahualcóyotl, Estado de México

Isabel

PRESENTE

El Instituto Electoral de la Ciudad de México (Instituto Electoral) comprometido con la ciudadanía de la entidad y con potenciar el ejercicio de sus derechos políticos-electorales, ha realizado permanentemente trabajos de investigación tendentes a conocer y analizar las diversas tecnologías que permitan la modernización, automatización y reducción de costos, de los procesos electorales y de participación ciudadana, específicamente para la recepción y cómputo de votos y opiniones.

Como parte de las actividades institucionales de este año, el Instituto Electoral realizará la Elección de Comisiones de Participación Comunitaria 2020 y la Consulta de Presupuesto Participativo 2020 y 2021, en la cuales, se utilizará el Sistema Electrónico por Internet (SEI) como un mecanismo adicional para recabar los votos y las opiniones de dichos ejercicios, por tal motivo y con la intención de incrementar el nivel de confianza en la ciudadanía, este Instituto tiene considerado llevar a cabo una auditoría informática al citado sistema.

Considerando que el 28 de octubre de 2019, este Instituto Electoral aprobó el Estudio de viabilidad técnica, operativa y financiera para proponer el uso del Sistema Electrónico por Internet para recabar los votos en las demarcaciones Cuauhtémoc y Miguel Hidalgo de forma presencial y remota.

En tal virtud, se extiende una cordial invitación para que participe en el proceso de selección de Auditores Externos para la Elección 2019 y en la Consulta Ciudadana 2020. En el caso de que sea de su interés, le solicito de la manera más atenta y de no existir inconveniente; se envíe por escrito y de forma electrónica a la dirección utsi@iecm.mx su propuesta Técnico-Económica, a más a tardar el 7 de febrero del presente año.

INSTITUTO ELECTORAL CIUDAD DE MÉXICO

UNIDAD TÉCNICA DE SERVICIOS INFORMÁTICOS

Ciudad de México, a 4 de febrero de 2020
IECM/UTSI/036/2020

Lo anterior para dar continuidad a la invitación realizada mediante oficio IECM/UTSI/082/2019 para participar como Auditor Externo, así como su respuesta a través de oficio No IFSAR/CTA/089/2019 en el que manifiesta el interés en participar (anexo copia de los oficios citados)

A efecto de tener los elementos necesarios para elaborar la propuesta referida, me permito indicar las ligas de Internet, donde se podrán consultar la convocatoria y la guía de implementación del Sistema Electrónico por Internet. Así mismo anexo los requerimientos que se deberán atender para la Auditoría de mérito.

- https://www.iecm.mx/www/taip/cg/acu/2019/IECM-ACU-CG-079-2019.pdf
- https://www.iecm.mx/www/taip/cg/acu/2019/IECM-ACU-CG-078-2019.pdf

Sin otro particular, reciba un cordial saludo

ATENTAMENTE

Lic. Oscar Alejandro Rodríguez Paz
Titular de Unidad Técnica de Servicios Informáticos

C.P. Mtro. Mario Velázquez Miranda, Consejero Presidente del Instituto Electoral de la Ciudad de México. Presente
Mtra. Myriam Alarcón Reyes, Presidenta de la Comisión de Organización Electoral y Geoestadística del Instituto Electoral de la Ciudad de México. Presente
Mtra. Carolina del Angel Cruz, Enlace de la Secretaría Ejecutiva, Dirección de Organización Electoral y Geoestadística del Instituto Electoral de la Ciudad de México. Presente
Mtra. Gabriela Williams Salazar, Integrante de la Comisión de Organización Electoral y Geoestadística del Instituto Electoral de la Ciudad de México. Presente
Lic. Rubén Geraldo Venegas, Secretario Ejecutivo del Instituto Electoral de la Ciudad de México. Presente
Mtro. Alejandro Fidencio González Hernández, Secretario Administrativo del Instituto Electoral de la Ciudad de México. Presente
Lic. Cecilia A. Hernández Cruz, Titular de la Unidad Técnica de Vinculación con Organismos Externos del Instituto Electoral de la Ciudad de México. Presente
Archivo

OARP/NFP.FM.

INSTITUTO ELECTORAL CIUDAD DE MÉXICO

UNIDAD TÉCNICA DE SERVICIOS INFORMÁTICOS

ACUSE

Ciudad de México, a 4 de febrero de 2020
IECM/UTSI/036/2020

Dr. Sergio López Ayllón
Director General
Centro de Investigación y Docencia Económicas
Carretera México-Toluca 3655
Sta. Fe, Altavista
C.P. 01210, Alvaro Obregón
Ciudad de Mexico

CIDE DIRECCION GENERAL
RECIBIDO

PRESENTE

El Instituto Electoral de la Ciudad de México (Instituto Electoral) comprometido con la ciudadanía de la entidad y con potenciar el ejercicio de sus derechos políticos-electorales, ha realizado permanentemente trabajos de investigación tendentes a conocer y analizar las diversas tecnologías que permitan la modernización, automatización y reducción de costos, de los procesos electorales y de participación ciudadana, específicamente para la recepción y computo de votos y opiniones.

Como parte de las actividades institucionales de este año, el Instituto Electoral realizará la Elección de Comisiones de Participación Comunitaria 2020 y la Consulta de Presupuesto Participativo 2020 y 2021, en la cuales, se utilizará el Sistema Electrónico por Internet (SEI) como un mecanismo adicional para recabar los votos y las opiniones de dichos ejercicios; por tal motivo y con la intención de incrementar el nivel de confianza en la ciudadanía, este Instituto tiene considerado llevar a cabo una auditoría informática al citado sistema.

Considerando que el 28 de octubre de 2019, este Instituto Electoral aprobó el Estudio de viabilidad técnica, operativa y financiera para proponer el uso del Sistema Electrónico por Internet para recabar los votos en las demarcaciones Cuauhtémoc y Miguel Hidalgo de forma presencial y remota.

En tal virtud, se extiende una cordial invitación para que participe en el proceso de selección de Auditores Externos para la Elección 2019 y en la Consulta Ciudadana 2020. En el caso de que sea de su interes, le solicito de la manera más atenta y de no existir inconveniente; se envíe por escrito y de forma electrónica a la dirección utsi@iecm.mx su propuesta Técnico-Económica, a más a tardar el 7 de febrero del presente año.

INSTITUTO ELECTORAL CIUDAD DE MÉXICO

UNIDAD TÉCNICA DE SERVICIOS INFORMÁTICOS

Ciudad de México, a 4 de febrero de 2020
IECM/UTSI/036/2020

A efecto de tener los elementos necesarios para elaborar la propuesta referida; me permito indicar las ligas de Internet, donde se podrán consultar la convocatoria y la guia de implementación del Sistema Electrónico por Internet. Así mismo anexo los requerimientos que se deberán atender para la Auditoria de mérito.

- https //www.iecm mx/www/taip/cg/acu/2019/IECM-ACU-CG-079-2019.pdf
- https //www.iecm mx/www/taip/cg/acu/2019/IECM-ACU-CG-078-2019.pdf

Sin otro particular, reciba un cordial saludo

ATENTAMENTE

Lic. Oscar Alejandro Rodríguez Paz
Titular de Unidad Técnica de Servicios Informáticos

C.P. Mtro. Mario Velázquez Miranda.- Consejero Presidente del Instituto Electoral de la Ciudad de México.- Presente
Mtra. Myriam Alarcón Reyes.- Presidenta de la Comisión de Organización Electoral y Geoestadística del Instituto Electoral de la Ciudad de México.- Presente
Mtra. Carolina del Ángel Cruz.- Integrante de la Comisión de Organización Electoral y Geoestadística del Instituto Electoral de la Ciudad de México.- Presente
Mtra. Gabriela Williams Salazar.- Integrante de la Comisión de Organización Electoral y Geoestadística del Instituto Electoral de la Ciudad de México.- Presente
Lic. Rubén Geraldo Venegas.- Secretario Ejecutivo del Instituto Electoral de la Ciudad de México.- Presente
Mtro. Alejandro Fidencio González Hernández.- Secretario Administrativo del Instituto Electoral de la Ciudad de México.- Presente
Lic. Cecilia A. Hernández Cruz.- Titular de la Unidad Técnica de Vinculación con Organismos Externos del Instituto Electoral de la Ciudad de México.- Presente
Archivo

GARP/EFR/EM

Sistema de Auditoría

Rev. 1/2019

INSTITUTO ELECTORAL CIUDAD DE MÉXICO

ACUSE

UNIDAD TÉCNICA DE SERVICIOS INFORMÁTICOS

Ciudad de México, a 4 de febrero de 2020
IECM/UTSI/036/2020

Dra. Marcela Peñaloza Báez
Directora de Colaboración y Vinculación de la Dirección General Cómputo y de Tecnologías de Información y Comunicación de la Universidad Nacional Autónoma de México
Ciudad Universitaria, Circuito Exterior S/N Coyoacán
C.P. 04510 Ciudad de México

DIRECCIÓN GENERAL DE CÓMPUTO Y DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN
04 FEB 2020
RECIBIDO
Dirección de Colaboración y Vinculación

PRESENTE

El Instituto Electoral de la Ciudad de México (Instituto Electoral) comprometido con la ciudadanía de la entidad y con potenciar el ejercicio de sus derechos políticos-electorales, ha realizado permanentemente trabajos de investigación tendentes a conocer y analizar las diversas tecnologías que permitan la modernización, automatización y reducción de costos, de los procesos electorales y de participación ciudadana, específicamente para la recepción y cómputo de votos y opiniones.

Como parte de las actividades institucionales de este año, el Instituto Electoral realizará la Elección de Comisiones de Participación Comunitaria 2020 y la Consulta de Presupuesto Participativo 2020 y 2021, en la cuales, se utilizará el Sistema Electrónico por Internet (SEI) como un mecanismo adicional para recabar los votos y las opiniones de dichos ejercicios, por tal motivo y con la intención de incrementar el nivel de confianza en la ciudadanía, este Instituto tiene considerado llevar a cabo una auditoría informática al citado sistema.

Considerando que el 28 de octubre de 2019, este Instituto Electoral aprobó el Estudio de viabilidad técnica, operativa y financiera para proponer el uso del Sistema Electrónico por Internet para recabar los votos en las demarcaciones Cuauhtémoc y Miguel Hidalgo de forma presencial y remota.

En tal virtud, se extiende una cordial invitación para que participe en el proceso de selección de Auditores Externos para la Elección 2019 y en la Consulta Ciudadana 2020. En el caso de que sea de su interés, le solicito de la manera más atenta y de no existir inconveniente, se envíe por escrito y de forma electrónica a la dirección utsi@iecm.mx su propuesta Técnico-Económica, a más a tardar el 7 de febrero del presente año.

INSTITUTO ELECTORAL CIUDAD DE MÉXICO

UNIDAD TÉCNICA DE SERVICIOS INFORMÁTICOS

Ciudad de México, a 4 de febrero de 2020
IECM/UTSI/036/2020

lo anterior para dar continuidad a la invitación realizada mediante oficio IECM/UTSI/082/2019 para participar como Auditor Externo, así como su respuesta a través de oficio No TIC/DCV/042/2019 en el que manifiesta el interés en participar (anexo copia de los oficios citados).

A efecto de tener los elementos necesarios para elaborar la propuesta referida, me permito indicar las ligas de Internet donde se podrán consultar la convocatoria y la guía de implementación del Sistema Electrónico por Internet. Así mismo anexo los requerimientos que se deberán atender para la Auditoría de mérito.

- https://www.iecm.mx/www/taip/cg/acu/2019/IECM-ACU-CG-079-2019.pdf
- https://www.iecm.mx/www/taip/cg/acu/2019/IECM-ACU-CG-078-2019.pdf

Sin otro particular, reciba un cordial saludo.

ATENTAMENTE

Lic. Oscar Alejandro Rodríguez Paz
Titular de Unidad Técnica de Servicios Informáticos

c.c.p. Mtro. Mario Velázquez Miranda, [illegible] Presidente del Instituto Electoral de la Ciudad de México. Presente.
Mtra. Myrtain Atarcón Reyes, [illegible] del Instituto Electoral de la Ciudad de México. Presente.
Mtra. Carolina del Angel Cruz, [illegible] del Instituto Electoral de la Ciudad de México. Presente.
Mtra. Gabriela Williams Salazar, [illegible] del Instituto Electoral de la Ciudad de México. Presente.
Lic. Rubén Geraldo Venegas, [illegible] de la Ciudad de México. Presente.
Mtro. Alejandro Espinosa González Hernández, [illegible] del Instituto Electoral de la Ciudad de México. Presente.
Lic. Cecilia A. Hernández Cruz, [illegible] del Instituto Electoral de la Ciudad de México. Presente.
Archivo.

OARP/ [illegible]

NOTARIA [illegible]

INSTITUTO ELECTORAL CIUDAD DE MÉXICO

ACUSE

UNIDAD TÉCNICA DE SERVICIOS INFORMÁTICOS

Ciudad de México, a 4 de febrero de 2020
IECM/UTSI/036/2020

Dra. Ana Covarrubias Velasco
Coordinadora General Académica
Colegio de México
Carretera Picacho Ajusco 20 Ampliación
Fuentes del Pedregal
C.P. 14110, Tlalpan
Ciudad de México

EL COLEGIO DE MÉXICO

RECIBIDO

Coordinación General Académica

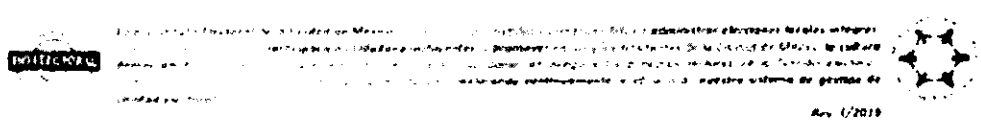
PRESENTE

El Instituto Electoral de la Ciudad de México (Instituto Electoral) comprometido con la ciudadanía de la entidad y con potenciar el ejercicio de sus derechos políticos-electorales, ha realizado permanentemente trabajos de investigación tendentes a conocer y analizar las diversas tecnologías que permitan la modernización, automatización y reducción de costos, de los procesos electorales y de participación ciudadana, específicamente para la recepción y computo de votos y opiniones.

Como parte de las actividades institucionales de este año, el Instituto Electoral realizará la Elección de Comisiones de Participación Comunitaria 2020 y la Consulta de Presupuesto Participativo 2020 y 2021, en la cuales, se utilizará el Sistema Electrónico por Internet (SEI) como un mecanismo adicional para recabar los votos y las opiniones de dichos ejercicios; por tal motivo y con la intención de incrementar el nivel de confianza en la ciudadanía, este Instituto tiene considerado llevar a cabo una auditoria informática al citado sistema.

Considerando que el 28 de octubre de 2019, este Instituto Electoral aprobó el Estudio de viabilidad técnica, operativa y financiera para proponer el uso del Sistema Electrónico por Internet para recabar los votos en las demarcaciones Cuauhtémoc y Miguel Hidalgo de forma presencial y remota.

En tal virtud, se extiende una cordial invitación para que participe en el proceso de selección de Auditores Externos para la Elección 2019 y en la Consulta Ciudadana 2020. En el caso de que sea de su interés, le solicito de la manera más atenta y de no existir inconveniente, se envíe por escrito y de forma electrónica a la dirección utsi@iecm.mx su propuesta Técnico-Económica a más a tardar el 7 de febrero del presente año.



INSTITUTO ELECTORAL
CIUDAD DE MÉXICO

UNIDAD TÉCNICA DE SERVICIOS INFORMÁTICOS

Ciudad de México, a 4 de febrero de 2020
IECM/UTSI/036/2020

A efecto de tener los elementos necesarios para elaborar la propuesta referida, me permito indicar las ligas de Internet, donde se podrán consultar la convocatoria y la guía de implementación del Sistema Electrónico por Internet. Así mismo anexo los requerimientos que se deberán atender para la Auditoría de mérito

- https //www iecm mx/www/taip/cg/acu/2019/IECM-ACU-CG-079-2019.pdf
- https //www iecm mx/www/taip/cg/acu/2019/IECM-ACU-CG-078-2019 pdf

Sin otro particular, reciba un cordial saludo

ATENTAMENTE

Lic. Oscar **Alejandro Rodríguez Paz**
Titular de Unidad Técnica de Servicios Informáticos

C.c.p. Mtro. Mario Velázquez Miranda, Consejero Presidente de la Junta del Instituto Electoral de la Ciudad de México. Presente
Mtra. Myriam Alarcón Reyes, Titular de la Unidad Técnica de Organización Electoral y Geoestadística del Instituto Electoral de la Ciudad de México. Presente
Mtra. Carolina del Ángel Cruz, Encargada de la Dirección de Organización Electoral y Geoestadística del Instituto Electoral de la Ciudad de México. Presente
Mtra. Gabriela Williams Salazar, Jefa de la Unidad Técnica de Organización Electoral y Geoestadística del Instituto Electoral de la Ciudad de México. Presente
Lic. Rubén Geraldo Venegas, Secretario Particular del Instituto Electoral de la Ciudad de México. Presente
Mtro. Alejandro Cuauhtémoc González Hernández, Secretario Administrativo del Instituto Electoral de la Ciudad de México. Presente
Lic. Cecilia A. Hernández Cruz, Titular de la Unidad Técnica de Asuntos Jurídicos y Lineamientos Electorales del Instituto Electoral de la Ciudad de México. Presente
Archivo

GARF/MFR/EM

Sistema de Gestión de Calidad

INSTITUTO ELECTORAL

Rev. 1 2019

INSTITUTO ELECTORAL CIUDAD DE MÉXICO

UNIDAD TÉCNICA DE SERVICIOS INFORMÁTICOS

Ciudad de México, a 4 de febrero de 2020
IECM/UTSI/036/2020

IPN ESCUELA SUPERIOR DE INGENIERÍA MECÁNICA Y ELÉCTRICA UNIDAD CULHUACAN SEP
04 FEB. 2020
DIRECCIÓN
RECIBIDO
ANEXOS SI (X) NO ( )

Mtro. Hector Becerril Mendoza
Director de la ESIME Culhuacán del Instituto Politécnico Nacional
Av. Santa Ana No. 1000
Col. Culhuacan Secc. 6, Coyoacán
C.P. 04440, Ciudad de México

PRESENTE

El Instituto Electoral de la Ciudad de México (Instituto Electoral) comprometido con la ciudadanía de la entidad y con potenciar el ejercicio de sus derechos políticos-electorales, ha realizado permanentemente trabajos de investigación tendentes a conocer y analizar las diversas tecnologías que permitan la modernización, automatización y reducción de costos, de los procesos electorales y de participación ciudadana, especificamente para la recepción y cómputo de votos y opiniones.

Como parte de las actividades institucionales de este año, el Instituto Electoral realizará la Elección de Comisiones de Participación Comunitaria 2020 y la Consulta de Presupuesto Participativo 2020 y 2021, en la cuales, se utilizará el Sistema Electrónico por Internet (SEI) como un mecanismo adicional para recabar los votos y las opiniones de dichos ejercicios, por tal motivo y con la intención de incrementar el nivel de confianza en la ciudadanía, este instituto tiene considerado llevar a cabo una auditoría informática al citado sistema.

Considerando que el 28 de octubre de 2019, este Instituto Electoral aprobó el Estudio de viabilidad técnica, operativa y financiera para proponer el uso del Sistema Electrónico por Internet para recabar los votos en las demarcaciones Cuauhtémoc y Miguel Hidalgo de forma presencial y remota.

En tal virtud, se extiende una cordial invitación para que participe en el proceso de selección de Auditores Externos para la Elección 2019 y en la Consulta Ciudadana 2020. En el caso de que sea de su interés, le solicito de la manera más atenta y de no existir inconveniente, se envíe por escrito y de forma electrónica a la dirección utsi@iecm.mx su propuesta Técnico-Económica a más a tardar el 7 de febrero del presente año.

INSTITUTO ELECTORAL CIUDAD DE MÉXICO

UNIDAD TÉCNICA DE SERVICIOS INFORMÁTICOS

Ciudad de México, a 4 de febrero de 2020
IECM/UTSI/036/2020

Lo anterior para dar continuidad a la invitación realizada mediante oficio IECM/UTSI/082/2019 para participar como Auditor Externo; así como su respuesta a través de oficio No. DC-1618/SEPI-0/2019 en el que manifiesta el interés en participar (anexo copia de los oficios citados).

A efecto de tener los elementos necesarios para elaborar la propuesta referida, me permito indicar las ligas de Internet, donde se podrán consultar la convocatoria y la guía de implementación del Sistema Electrónico por Internet. Así mismo anexo los requerimientos que se deberán atender para la Auditoría de mérito.

- ✓ https://www.iecm.mx/www/taip/cg/acu/2019/IECM-ACU-CG-079-2019.pdf
- ✓ https://www.iecm.mx/www/taip/cg/acu/2019/IECM-ACU-CG-078-2019.pdf

Sin otro particular, reciba un cordial saludo.

ATENTAMENTE

Lic. Oscar Alejandro Rodríguez Paz
Titular de Unidad Técnica de Servicios Informáticos

Mtro. Mario Velázquez Miranda [illegible] Instituto Electoral de la Ciudad de México. Presente
Mtra. Mynam Alarcon Reyes [illegible] Comisión de Organización Electoral y Geoestadística del Instituto Electoral de la Ciudad de México. Presente
Mtra. [illegible] Comisión de Organización Electoral y Geoestadística del Instituto Electoral de la Ciudad de México. Presente
Mtra. Gabriela Woldenberg Salazar [illegible] Comisión de Organización Electoral y Geoestadística del Instituto Electoral de la Ciudad de México. Presente
Lic. Rubén Geraldo Venegas [illegible] del Instituto Electoral de la Ciudad de México. Presente
Mtro. Alejandro Fidencio González Hernández Secretario Administrativo del Instituto Electoral de la Ciudad de México. Presente
Lic. Cecilia A. Hernández Cruz Titular de la Unidad Técnica de Vinculación con Organismos Externos del Instituto Electoral de la Ciudad de México. Presente
Archivo

CARPETA E Mc

[illegible]

Rev. 1/2019

INSTITUTO ELECTORAL
CIUDAD DE MÉXICO

UNIDAD TÉCNICA DE SERVICIOS INFORMÁTICOS

Ciudad de México, a 4 de febrero de 2020
IECM/UTSI/036/2020

Mtro. J. Rodrigo Serrano Vásquez
Abogado General
Universidad Autónoma Metropolitana
Prol. Canal de Miramontes No. 3855
Coapa, Ex. De San Juan de Dios
C.P. 14387, Tlalpan
Ciudad de México

432

14:10hrs. PM

RECIBIDO

PRESENTE

El Instituto Electoral de la Ciudad de México (Instituto Electoral) comprometido con la ciudadanía de la entidad y con potenciar el ejercicio de sus derechos políticos-electorales, ha realizado permanentemente trabajos de investigación tendentes a conocer y analizar las diversas tecnologías que permitan la modernización, automatización y reducción de costos, de los procesos electorales y de participación ciudadana, específicamente para la recepción y cómputo de votos y opiniones.

Como parte de las actividades institucionales de este año, el Instituto Electoral realizará la Elección de Comisiones de Participación Comunitaria 2020 y la Consulta de Presupuesto Participativo 2020 y 2021, en la cuales, se utilizará el Sistema Electrónico por Internet (SEI) como un mecanismo adicional para recabar los votos y las opiniones de dichos ejercicios, por tal motivo y con la intención de incrementar el nivel de confianza en la ciudadanía, este Instituto tiene considerado llevar a cabo una auditoría informática al citado sistema.

Considerando que el 28 de octubre de 2019, este Instituto Electoral aprobó el Estudio de viabilidad técnica, operativa y financiera para proponer el uso del Sistema Electrónico por Internet para recabar los votos en las demarcaciones Cuauhtémoc y Miguel Hidalgo de forma presencial y remota.

En tal virtud, se extiende una cordial invitación para que participe en el proceso de selección de Auditores Externos para la Elección 2019 y en la Consulta Ciudadana 2020. En el caso de que sea de su interés, le solicito de la manera más atenta y de no existir inconveniente; se envíe por escrito y de forma electrónica a la dirección utsi@iecm.mx su propuesta Técnico-Económica, a más a tardar el 7 de febrero del presente año.

Huizaches No. 25, Colonia Rancho Los Colorines, Tlalpan, C.P. 14386, Ciudad de México. Conmutador 5483-3800

INSTITUTO ELECTORAL
CIUDAD DE MÉXICO

UNIDAD TÉCNICA DE SERVICIOS INFORMÁTICOS

Ciudad de México, a 4 de febrero de 2020
IECM/UTSI/036/2020

A efecto de tener los elementos necesarios para elaborar la propuesta referida, me permito indicar las ligas de Internet donde se podrán consultar la convocatoria y la guia de implementación del Sistema Electrónico por Internet. Asi mismo anexo los requerimientos que se deberán atender para la Auditoria de mérito.

- https://www.iecm.mx/www/taip/cg/acu/2019/IECM-ACU-CG-079-2019.pdf
- https://www.iecm.mx/www/taip/cg/acu/2019/IECM-ACU-CG-078-2019.pdf

Sin otro particular, reciba un cordial saludo.

ATENTAMENTE

Lic. **Oscar Alejandro Rodríguez Paz**
Titular de Unidad Técnica de Servicios Informáticos

C.c.p. Mtro. Mario Velázquez Miranda, Consejero Presidente del Instituto Electoral de la Ciudad de México. Presente.
Mtra. Myriam Alarcón Reyes, Presidenta de la Comisión de Organización Electoral y Geoestadística del Instituto Electoral de la Ciudad de México. Presente.
Mtra. Carolina del Angel Cruz, Titular de la Dirección de Organización Electoral y Geoestadística del Instituto Electoral de la Ciudad de México. Presente.
Mtra. Gabriela Williams Salazar, Titular de la Unidad de Organización Electoral y Geoestadística del Instituto Electoral de la Ciudad de México. Presente.
Lic. Rubén Geraldo Venegas, Secretario Ejecutivo del Instituto Electoral de la Ciudad de México. Presente.
Mtro. Alejandro Fidencio González Hernández, Secretario Administrativo del Instituto Electoral de la Ciudad de México. Presente.
Lic. Cecilia A. Hernández Cruz, Titular de la Unidad Técnica de Vinculación con Organismos Externos del Instituto Electoral de la Ciudad de México. Presente.
Archivo.

AARO/KEP/LTM

Folio 115

UNAM
FES Aragón

FACULTAD DE ESTUDIOS SUPERIORES ARAGON
CENTRO TECNOLOGICO ARAGÓN

Oficio No. FESAR/CTA/025/2020
Asunto: ACEPTACIÓN DE LA INVITACION
ENTIDAD: INSTITUTO ELECTORAL DE LA CIUDAD DE MÉXICO

MTRO. OSCAR ALEJANDRO RODRÍGUEZ PAZ
TITULAR DE LA UNIDAD TÉCNICA DE SERVICIOS INFORMÁTICOS
P R E S E N T E

Nos permitimos agradecerle la invitación a participar en el proceso de selección de Auditores Externos para Elección 2019 y en la Consulta Ciudadana 2020, número de oficio. IECM/UTSI/036/2020, y manifestamos que aceptamos con todo gusto dicha invitación, por lo que anexamos a éste documento la propuesta Técnico-Económica.

Sin otro particular y gradeciendo la atención que sirva dar a la presente, le enviamos un cordial saludo

A T E N T A M E N T E
"POR MI RAZA HABLARÁ EL ESPÍRITU"
Nezahualcóyotl, Estado de México, a 5 de febrero de 2020
COORDINADOR

DR. JACINTO CORTÉS PÉREZ

c.c.p. Expediente
JCP'img

CENTRO TECNOLOGICO FES ARAGON
COORDINACIÓN
U.N.A.M.

UNAM
La Universidad de la Nación

UNIDAD TÉCNICA SERVICIOS INFORMÁTICOS

RECIBIDO

INSTITUTO ELECTORAL CIUDAD DE MÉXICO

UNAM FES Aragón

PROPUESTA TÉCNICO – ECONÓMICA PARA LA AUDITORÍA INFORMÁTICA A LA INFRAESTRUCTURA Y SOFTWARE DEL SISTEMA ELECTRÓNICO POR INTERNET (SEI) 2020 PARA EL INSTITUTO ELECTORAL DE LA CIUDAD DE MÉXICO.

I. OBJETIVO GENERAL

Realizar una auditoría informática al Sistema Electrónico por Internet (SEI) 2020, del Instituto Electoral de la Ciudad de México conforme al reglamento de elecciones aprobado mediante acuerdo del Consejo General del Instituto Nacional Electoral. No. INE/CG661/2016.

De forma general, la auditoría deberá determinar si el (SEI) 2020 es seguro, robusto, confiable y realiza exclusivamente las operaciones y funciones para las cuales fue diseñado, de acuerdo con el manual de usuario garantizando la integridad en el procesamiento de toda la información.

II. OBJETIVOS ESPECÍFICOS

1. Revisar el sistema informático y los correspondientes aplicativos desarrollados específicamente para el SEI en términos de funcionalidad. La auditoría deberá determinar, mediante un análisis detallado del código, que los aplicativos SEI realizan las funciones descritas en el manual de usuario y solamente esas, es decir, el programa solamente hace lo que se espera de él, procesando transparente y correctamente la información desde su origen hasta la publicación.

   Dentro de los aspectos a revisar en el rubro de calidad del sistema se incluyen:

   1. Verificación de la arquitectura del sistema.
   2. Controles adecuados en la entrada de datos.
   3. Almacenamiento y restauración de datos.
   4. Implementación de bitácoras en el procesamiento de datos sensibles.
   5. Cumplimiento en buenas prácticas de codificación basado en estándares en donde se protejan los componentes por medio de encapsulamiento niveles de acceso y buena implementación de estructuras de control.

6. Manejo de errores.
7. Evaluación de desempeño.

2. Probar todas los aplicativos desarrallados especificamente para el SEI en términos de funcionalidad.

3. Analizar las posibles vulnerabilidades de la infraestructura tecnológica del SEI.

4. Ejecutar pruebas de denegación de servicios (DoS) para comprobar la robustes y disponibilidad del servicio.

5. Diseñar y ejecutar pruebas de Penetración (PenTest) al sistema e infraestructura que soporta al sistema SEI.

III. ALCANCES

1. La auditoría se realizará cuando el SEI 2020 alcance el 100% de avance en su desarrollo.

2. Se realizará una planificación de la auditoria, identificando claramente las recursos materiales y técnicos necesarios para llevarla a cabo.

3. La auditoría se realizará con base en una metadologia estandarizada internacionalmente que incluya procedimientos para comprobar los controles a revisar; así como formatos y contenido de los reportes que se deriven de ésta.

La Metodología utilizada cubrirá las siguientes etapas y actividades:

Para la auditoría a las aplicaciones de software.

La revisión de:

- Control de ingreso (entrada) de los datos al sistema de aplicación en funcionamiento, así como los demás perfiles del sistema para asegurar que se cumpla con la segregación de funciones (administración, dar de alta usuarias, maneja de contraseñas), para asegurar que cada transacción a ser procesada cumpla con los siguientes requisitos:

INSTITUTO ELECTORAL
CIUDAD DE MÉXICO

UNAM
FES
Aragón

A. Validar la entrada de datos al sistema.
B. Procesar solamente datos válidos y autorizados.
C. Ingresar los datos una vez por cada transacción.

Se revisará que:

- Las pantallas de captura de datos estén diseñadas en forma consistente con los documentos fuente.
- En el ingreso de los datos, la aplicación tenga mensajes de ayuda, con el fin de facilitar su captura.
- Restringir el acceso de los usuarios a las diferentes opciones de la aplicación.
- Verificar los procedimientos de asignación de permisos a usuarios de la base de datos.
- Verificar en cada pantalla de captura, que los campos de los datos importantes sea de obligatoria digitación.
- En toda la aplicación, cada campo tenga el formato de datos apropiado.
- En la captura o modificación de datos críticos tengan una pista (log o bitácora) donde se identifique lo siguiente: nombre del usuario, fecha y hora, valor del campo y donde se realizo la transacción así como qué tipo de operación realizó ese cambio.
- Verificar que las bitácoras (logs) de la aplicación puedan ser revisados por los responsables para investigar accesos y manipulaciones no autorizadas.
- Verificar la integridad de las bitácoras (logs) y que cuenten con la protección de escritura solamente para los sistemas y de lectura solamente para segregar la función de auditoría y revisión.
- En la captura numérica se controle la correcta digitación de cantidades. En la captura de información se cuente con los controles adecuados para la disminución de errores de captura.
- La aplicación permita imprimir en pantalla listados de datos que han sido ingresados, validados y procesados, para que estos sean revisados por los usuarios, con el propósito de verificar el avance en la conclusión del total de los datos.
- Si en el ingreso de los datos hay un rechazo por el sistema; que ese dato sea analizado y corregido por los usuarios

- Validar los procedimientos de excepciones tales como: una acta tenga problemas de origen, datos ilegibles, número de votos mayor que la lista nominal, casillas zapato[1], etcétera.
- Revisar el funcionamiento del procedimiento del programa que valida al momento que se detecte un error de captura.

Dentro del área de control de entrada de datos a los sistemas gestores de bases de datos se verificarán los siguientes puntos:

A. Transacciones en línea.
B. Usuario y operador.
C. Terminal o dispositivo de entrada de datos.

A. Transacciones en línea.

Disponer de los siguientes mecanismos de control:

- Manejo de transacciones erróneas o incompletas de Base de datos.
- Asegurar la consistencia e integridad de los datos de las transacciones en la base de datos.
- Comprobar el procedimiento de desconexión al servidor central y el restablecimiento de la conexión, asegurando la correcta sincronización de las transacciones en las bases de datos.
- Asegurar que existan mecanismos de detección de errores y de corrección de los mismos.
- Asegurar que existan mecanismos de transacciones en base de datos que provean de pistas de auditoría para pruebas posteriores y que los mismos sirvan como medio de evidencia ante requerimientos legales o regulatorios.
- Mantener un conteo de transacciones ingresadas para comparar con la información recibida en la base de datos central.
- Prever la formulación de informes sobre tipos de transacciones desarrolladas.
- Mantener continuidad en el procedimiento de captura en caso de in-operatividad de alguna terminal.

[1] Casillas donde el 100% de los votos son para un mismo partido.

- Verificar la existencia de manuales y procedimientos de entrenamiento (o equivalentes).

B. Usuario y Operador de entrada de datos.

Verificar que el sistema cuente con los siguientes controles:

- Minimizar la posibilidad de que se cometan errores humanos durante la captura de datos.
- Asegurar que las funciones que ejecutan los operadores de datos sobre áreas reservadas se ajustan a las políticas y prácticas de control de la organización.
- Permitir el ingreso de datos, consulta y actualización de archivos únicamente a personas propiamente autorizadas e identificadas.
- Asegurar el procedimiento para mantener la confidencialidad de las contraseñas para las llaves de cifrado de datos y de las bases de datos.
- Asegurar la confidencialidad en el manejo y distribución de llaves de cifrado de datos y contraseñas.

C. Terminal o dispositivo de entrada de datos.

Objetivos:

- Asegurar que el sistema sea utilizado por operadores autorizados y desde lugares autorizados.
- Resguardar con seguridad el área destinada a los servidores.
- Asegurar que antes de efectuar una conexión e iniciar una sesión de transmisión de datos se verifique que la respectiva "terminal" sea autenticada con algún mecanismo.
- Asegurar la autenticidad del operador/usuario.

Para la auditoría a la infraestructura de hardware y software que soporta a las aplicaciones.

A. Reconocimiento de la red externa

Identificar los puntos de acceso y consulta que tiene el instituto para el público en general a fin de ubicar la infraestructura que lo soporta. En este proceso se hará uso de herramientas de mapeo e identificación de red estableciendo los límites de la infraestructura de comunicaciones para desarrollar un modelo para las siguientes etapas:

- Identificación de puntos con presencia en Internet.
- Obtención de registros públicos (NIC).
- Enumeración de nodos externos.
- Enumeración de servicios externos.
- Enumeración de manejadores de base de datos.
- Análisis del contexto general del instituto.

B. Obtención de equipo objetivo

Basados en los resultados de la etapa anterior se enumerará y conocerán los nodos y servicios activos, así como los que se encuentran en modalidad silenciosa. A partir de esta información, se elaborará un diagrama que registre sistemas operativos, aplicaciones operativas y dispositivos de red alcanzables.

- Documentación de los nodos activos.
- Documentación de los nodos ocultos.
- Enumeración de los nodos confiables.
- Determinar los tipos de sistemas operativos.
- Determinar la configuración de los sistemas operativos.
- Determinar los tipos de manejadores de bases de datos.

C. Valoración de vulnerabilidades

Se realizarán pruebas tanto automatizadas como manuales para obtener acceso a todos los recursos de información de los dispositivos localizados como objetivo en la etapa anterior:

- Identificar riesgos utilizando herramientas de libre uso o propietarias.
- Identificar riesgos en sistemas operativos y en bases de datos.

INSTITUTO ELECTORAL
CIUDAD DE MÉXICO

UNAM FES Aragón

- Identificar exploits de acuerdo a las vulnerabilidades encontradas

D. Pruebas de penetración

Las pruebas se realizarán utilizando las metodologías mencionadas en los alcances. Se analizará la seguridad de la red desde el punto de vista externo (Internet), desde la red local del instituto (LAN), desde una línea de suscriptor digital asimétrico (ADSL) y mediante la utilización de enlaces privados del Instituto; todas ellas sin el conocimiento previo de la topología de red (caja negra).
Se realizarán estas pruebas con la intención de mostrar el grado de exposición de las aplicaciones, bases de datos e infraestructura del Instituto. Las pruebas incluirán:

- Pruebas de "caja negra" y "caja blanca".
- Pruebas de "man in the middle".
- Pruebas a las instancias de base de datos.
- Pruebas de penetración para VMware (en caso de ser utilizado).
- Pruebas de Active Directory injection.
- Pruebas de penetración hacia los aplicativos.

- Depositar banderas en los objetivos que haya sido posible acceder sin afectar la operación y sin modificar la información alcanzada.
- Evidenciar las vulnerabilidades en aplicaciones, base de datos e infraestructura de TI que permitan acceso o negación de los servicios.
- Integrar pruebas de penetración a la infraestructura de la red inalámbrica del Instituto, que como mínimo contenga lo siguiente:

- Obtención de SSID.
- Obtención de marca de AP.
- Obtención de APs abiertos
- Obtención de tipo de cifrado TKIP (Temporal Key Integrity Protocol) y AES (Advanced Encryption Standard).
- Obtención de autenticación WEP y WPA.
- Pruebas de ruptura de cifrado.
- Direccionamiento de la red Wireless
- Identificación de broadcast de SSID.
- Búsqueda de AP sin SSID.

- Validación de tipo de cifrado.
- Captura de tráfico cifrado.

IV. EJECUCIÓN DE LA REVISIÓN

Infraestructura - Verificación de la infraestructura de cómputo y comunicaciones donde operará el SEI con las siguientes actividades:

- Verificar la infraestructura de cómputa y comunicaciones que se encuentre alojada en el Centro de Cómputo propiedad del instituto.
- Verificar la configuración de la infraestructura de cómputo y comunicaciones que se encuentre alojada en la nube(de ser el caso).
- Comprobar que la arquitectura de la infraestructura de cómputo y comunicaciones corresponda a las necesidades del SEI.
- Verificar que los parches y actualizaciones de los sistemas operativos se encuentren estables; acorde a las necesidades del SEI.
- Comprobar que existan procedimientos que permitan asegurar los accesos físicos y lógicos a la infraestructura de cómputo y comunicaciones del instituto, además del acceso lógico a la infraestructura ubicada en la nube.

Software – Revisión del software que operará en el SEI con las siguientes actividades:

- Asegurar que la integridad de la información se mantenga en todo momento en el SEI.

- Verificar que el desarrollo del SEI cumpla por lo menos un proceso estándar de Ingeniería de Software: Metodología en cascada, RUP, TSPi, SCRUM, Extreme Programming o semejante.
- Revisión del sistema informático y todos los aplicativos desarrollados utilizando información del OWASP (www.owasp.org), la cual es una organización que provee información de cómo construir un ambiente de pruebas y de técnicas de verificación que se deben usar en el desarrollo de aplicaciones WEB, teniendo como objetivo

INSTITUTO ELECTORAL
CIUDAD DE MÉXICO

UNAM FES Aragón

principal es desarrollar aplicaciones seguras, con base en lo que se considera las mejores practicas de programación a la fecha

- Las técnicas de verificación serán realizadas empleando software Open Source y/o propietario, para implementar el checklist de acuerdo al OWASP, que a continuación se presenta:

Authentication Session Management	OWASP-AUTHSM-001	Tiempo de Sesion	Asegurar que la sesión de autenticación tenga una adecuada longitud en con el fin de prevenir que alguien pueda adivinar alguna sesión ya autenticada
	OWASP-AUTHSM-002	Timeout de sesión	Asegurarse que la autenticación solo sea valida por un periodo de tiempo
	OWASP-AUTHSM-003	Reuso de sesión	Asegurar que los valores de la Autenticación no sean válidos cuando el usuario se mueve de una sesión protegida (https) a una no protegida (http)
	OWASP-AUTHSM-004	Propósito de sesión	Asegurar que la sesión sea invalidada por cuando el usuario se salida de la aplicación
	OWASP-AUTHSM-005	Formato de los valores de sesión	Asegurarse que los valores de autenticación no sean permanentes y que estos no sean escritos en ninguna parte del cache o historial de navegación
	OWASP-CM-006	Métodos HTTP	Asegurarse que la aplicación soporte los métodos GET y DELETE
	OWASP-CM-002	Sitios hospedados virtualmente	Determinar si el sitio es hospedado virtualmente
	OWASP-CM-003	Vulnerabilidades conocidas / parches de seguridad	Verificar que los sistemas operativos tengan los últimos parches de seguridad.
	OWASP-CM-004	Archivos de Respaldo	Asegurar que no existe acceso a archivos de respaldo o archivos de configuración de la aplicación públicamente
	OWASP-CM-004	Configuración del servidor	Asegurarse que no existan configuraciones por defecto del servidor
AppDOS	OWASP-AD-001	"Flooding" de Aplicación	Asegurarse que la aplicación sea resistente cuando se realicen grandes cantidades de tráfico
	OWASP-AD-010	Bloqueo de Aplicación	Asegurarse que un atacante no pueda provocar que alguna cuenta sea bloqueada
Autorización	OWASP-AC-002	Análisis de Navegación	Asegurar que la aplicación no permita la revisión de archivos de sistema de información así como el directorio no pueda tener acceso a archivos privilegiados
	OWASP-AC-011	Autorización	Asegurar que la aplicación haga una correcta autorización después de la autenticación de usuarios
	OWASP-AC-008	Manipulación de parámetros de Autenticación	Asegurar que los usuarios no puedan modificar su "rol" de cada
	OWASP-AC-014	Autenticación de páginas/funciones	Verificar si es posible acceder a páginas que requieren autenticación
	OWASP-AC-015	Ambiente de Aplicación	Verificar que cuando el usuario requiera hacer ciertas acciones antes de hacer otras, estas se realicen por completo
Authentication	OWASP-AUTHN-001	Autenticación por HTTPS	Verificar que las Autenticaciones sean cifradas al menos por SSL
	OWASP-AUTHN-002	Sobrepasar la Autenticación	Asegurar que no se pueda sobrepasar los métodos de autenticación.
Authentication Flow	OWASP-AUTHN-003	Envió de credenciales de Autenticación por canal encriptado	Asegurarse que el usuario y contraseña sean enviados en un canal seguro (cifrado)
	OWASP-AUTHN-004	Cuentas por defecto	Verificar que no se usen cuentas y password por defecto
	OWASP-AUTHN-005	Usuarios	Asegurar que el usuario no este bloqueado y que en caso de ser así que
	OWASP-AUTHN-006	Calidad de Credenciales	Asegurar que la complejidad de las credenciales sea la correcta.

INSTITUTO ELECTORAL
CIUDAD DE MÉXICO

UNAM FES Aragón

	OWASP-AUT-IN-007	Reinicio de contraseñas	Asegurarse que el usuario responda al menos a una pregunta secreta antes de que la contraseña pueda ser modificada.
	[redacted]	[redacted]	[redacted]
	OWASP-AUTHN-009	Estructura de la contraseña	Asegurarse que la contraseña está bien construida y que al menos use un carácter especial y que la autenticación no pueda ser sobrepasada usando estos caracteres.
	[redacted]	[redacted]	[redacted]
	OWASP-CM-005	Componentes del servidor web	Asegurar que ningún componente de servidor web como apache, tomcat, front page, etc. o módulo de estos presenten que el servidor este vulnerable.
	[redacted]	[redacted]	[redacted]
	OWASP-CM-007	Aplicaciones y librerías cargadas por defecto	Verificar que no se estén cargando módulos por defecto de algunas aplicaciones y librerías de programación.
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	OWASP-IM-001	Mensajes de Errores de la aplicación	Asegurar que los errores que regresa la aplicación no pueden ser usados por un atacante para realizar una fechoría
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	OWASP-IM-001	Errores de Aplicaciones	Asegurar que los errores que regresa la aplicación no pueden ser usados por un atacante para realizar una fechoría
[redacted]	[redacted]	[redacted]	[redacted]
	OWASP-DP-002	Aseguro de Datos	Asegurar que los recursos mantengan el CIA (Confidencialidad, Integridad, Autenticidad)

[redacted]	[redacted]	[redacted]	[redacted]
	OWASP-DP-004	Metodos de intercambio de SSL KEY	Asegurar que el servidor web no acepte intercambio de llaves de autenticación indefinidamente
	[redacted]	[redacted]	[redacted]
	OWASP-DP-006	Tuneles de las Rutas SSL	Asegurar que el sitio mantenga un tunnels apropiado de la llave SSL
	[redacted]	[redacted]	[redacted]
[redacted]	OWASP-IV-001	Inyección de scripts	Asegurar que la Aplicación no acepte entradas que no puedan procesar
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	OWASP-IV-003	Inyección de comandos de SO	Asegurar que la aplicación no permita la inyección de comandos de sistema operativo desde la interfaz de usuario
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	OWASP-IV-005	Cross Site Scripting	Asegurar que la aplicación no permita mostrar o reflejar scripts maliciosos

INSTITUTO ELECTORAL
CIUDAD DE MÉXICO

UNAM
FES
Aragón

- Revisión de sistema informático:
  - Se deben revisar los siguientes activos que conforman el sistema informático del Programa, en términos de desempeño funcionalidad, seguridad y gestión:
  - Se deberán validar los aplicativos que conforman el sistema SEI consiste en la compilación y firma de los aplicativos auditados.
    - Base de datos.
    - Servidores WEB.
    - Equipos de comunicaciones y balanceadores de carga.
    - Equipos de seguridad, como firewall, antivirus, etc.
    - Servidores de transferencia segura de archivos.
    - Equipo personal.
    - Servidores.
    - Servidor Web Institucional.
  - Se deberán evaluar los siguientes controles de gestión:
    - Administración de incidentes y problemas.
    - Operaciones y respaldos.
    - Controles de acceso a infraestructura y aplicaciones.
    - Control de cambios.
  - Seguridad física del Centro de Cómputo, ubicado en la Unidad de Informática del IECM y en los Centros de Acopio y Transmisión de Datos distritales.
  - Seguridad en telecomunicaciones.
- Verificar que las funcionalidades del SEI, contengan por lo menos el almacenamiento de bitácoras; con el objetivo de que se puedan demostrar los estados en los que se encuentra en cada momento el sistema; lo anterior para solucionar posibles incidentes a presentarse.
- Verificar que el SEI contenga un catalogo de errores con su respectiva acción correctiva.
- Verificar que existan procedimientos para el control de cambios de requerimientos en donde se documenten las solicitudes de cambio de funcionalidad y su respectiva aprobación.
- Verificar que existan procedimientos para el control de cambios de código fuente y administración de versiones del sistema SEI.
- Comprobar que el SEI, en su caso tenga el licenciamiento requerido para su operación.
- Verificar que los perfiles de seguridad de los usuarios y/o de acceso a la base de datos, respondan únicamente a las actividades para las cuales fueron creados.

- Los tipos de vulnerabilidades que se intentarán explotar en aplicativos de los portales externos serán:

    - SQL Injection.
    - Cross Site Scripting.
    - Errores en las aplicaciones.
    - Errores en los patrones de base de datos.
    - Directorios ocultos.
    - LDAP Injection.
    - Command Injection.
    - Buffer overflow.
    - Manipulación de parámetros http.
    - Corrupción de archivos.
    - Envenenamiento de Cookies.

- Realizar pruebas en las aplicaciones de los portales que sean necesarias para identificar:

    - Riesgos de seguridad.
    - URLs escaneadas.
    - URLs vulnerables.
    - Causas de los problemas de seguridad clasificados por tipo de amenaza.
    - Responsables de mitigación por cada uno de los problemas de seguridad encontrados durante las pruebas.
    - Tareas necesarias para la mitigación de los problemas de seguridad encontrados.

En caso de obtener acceso a algún servidor de bases de datos o servidor interno, se enumerarán los manejadores de bases de datos que se puedan "ver", el punto desde donde se tuvo acceso y se intentó comprometerlos. Toda la información a la que se tenga acceso, o bien, se obtenga a partir de los resultados de la prueba.

- Realizar el análisis de vulnerabilidades en la infraestructura tecnológica del SEI y contemplará lo siguiente:
    - Ejecución de herramientas automatizadas de búsqueda de vulnerabilidades.
    - Pruebas de inyección de código malicioso.

INSTITUTO ELECTORAL CIUDAD DE MÉXICO

UNAM FES Aragón

- Pruebas de penetración internas y externas que realicen pruebas de acceso a los diversos recursos del sistema informático.
- Análisis de código estático que consistirán en técnicas de análisis de código fuente.
- Pruebas de código dinámico sobre la aplicación en ejecución.

V. EJECUCIÓN DE LAS PRUEBAS

Para la realización de las pruebas, se empleará la metodología OSSTMM (Open Source Security Testing Methodology Manual).

Las pruebas se realizarán en dos periodos de tiempo:

- Primera: Previo y durante el primer simulacro.
- Segunda: Una vez solventados los posibles hallazgos encontrados en el primer periodo de pruebas.

En el caso de requerir más pruebas para fortalecer el SEI se realizarán conforme lo determinen el instituto y el auditor.

Se realizarán las pruebas en el sitio central donde operará el SEI y de forma remota en el caso de las pruebas de penetración y busqueda de vulnerabilidades.

Las pruebas que se ejecutarán para el SEI son:

- Pruebas de denegación de servicio: en el caso de encontrar hallazgos estos serán documentados con las evidencias respectivas para su mitigación.

- Pruebas de vulnerabilidad - se evidenciará y documentará el grado de visibilidad y el nivel de exposición ante ciertos riesgos de inclusión de código malicioso, o algún otro ataque controlado comprobando así la efectividad de la prueba. Esto es, que para considerar que una vulnerabilidad fue exitosa es necesario contar con la bandera o evidencia de intrusión.

- Escaneo de puertos - identificando así las sackets del SEI; los cuales deberán ser exclusivamente las necesarias para atender los servicios solicitadas.

- Pruebas de estrés a las aplicacianes que se utilicen en el SEI; identificando así los siguienles umbrales de riesgo: alto, moderadc, menar, baja.

Las pruebas se realizarán ante das modalidades:

- *"Caja negra"* - Para los sistemas expuestas a Internet.
- *"Caja blanca"* - Para los sistemas internos que operan en el SEI.

VI. DEL USO DE EQUIPO POR PARTE DEL AUDITOR

Todo equipo de cómputo propiedad del auditar que requiera conectarse a la infraestructura de red del instituto, estará protegido y actualizado contra cádiga maliciasa, virus, troyanas, etc., y cumplirá con las políticas de seguridad para equipos de terceros.

Tadas las herramientas y software utilizado para la auditaria deben ser del ente auditar, el IECM no proparcianará ningún tipa de licenciamienta para el levantamienta de dicha auditoria; tado el software instalada por parte de la empresa auditora será removida al final de la auditaria.

VII. DE LA PRESTACIÓN DEL SERVICIO

El auditor designará de entre su persanal técnica certificado en CISA de ISACA, al menos a dos especialistas en camputación a infarmática, con categaria de académico de tiempo completo y a estudiantes destacados de las niveles de licenciatura, maestria y/o doctarado ae dicha especialidad, asi camo otros académicos del área de computación para que participen en el desarrallo y cumplimienta del presente canvenia.

El auditar presentará la planeación de la auditaria, identificando claramente su alcance, así coma las recursas materiales y técnicos necesarios para llevarla a cabo, parte de la cual ya se encuentra plasmada en la presente propuesta;

INSTITUTO ELECTORAL
CIUDAD DE MÉXICO

UNAM FES Aragón

El auditor redactará la metodología de la auditoría incluyendo procedimientos y enfoque para verificar y comprobar los controles a revisar así como el formato y contenido de los reportes que se deriven de esta; la metodología estará basada en OSSTMM, los casos de pruebas de OSSTMM se agrupan en cinco (5) diferentes áreas que en conjunto prueban:

1. Robustez de los controles implementados para la seguridad de la información y de los datos.
2. Los controles implementados para la infraestructura de cómputo y de comunicaciones, de redes inalámbricas y dispositivos móviles.
3. Los controles para la detección de intentos de ataques de ingeniería social.
4. Los niveles de concientización en relación a los temas de seguridad informática en el personal de una organización.
5. Los controles de seguridad física de una organización.

Una vez que el auditor concluya con su revisión y haya presentado los resultados, deberá eliminar cualquier rastro en la infraestructura del instituto originado a raíz de las pruebas realizadas.

Sólo se podrán instalar, con previa autorización, aplicaciones de acceso remoto que sean claramente identificables como procesos activos y cuyos puertos y conexiones sean visibles. Estas aplicaciones deberán permanecer apagadas y desinstaladas mientras no estén en uso.
Queda prohibido modificar la configuración de un servidor, estación de trabajo o dispositivo de red. Si se llegase a requerir un cambio temporal éste deberá ser autorizado y programado con antelación. Al terminar la prueba controlada, se deberá confirmar que la configuración regresó a su estado original y que no hubo ninguna afectación.

Queda prohibido borrar, alterar o apagar el uso de las bitácoras (logs) en cualquier dispositivo, estación de trabajo o servidor. Se requiere que todas las acciones de auditor q eraen registradas de forma normal en las bitácoras existentes.

INSTITUTO ELECTORAL CIUDAD DE MÉXICO

UNAM FES Aragón

VIII. INFORME DE LA REVISIÓN Y RECOMENDACIONES

Los informes de la auditoría se emitirán en 2 momentos diferentes:

- Primero – Consistirá en los resultados emitidos durante el proceso de auditoria enfocada a los hallazgos y recomendaciones los cuales deben estar enfocados a garantizar la integridad de los resultados presentados.
- Segundo – Consistirá en el resultado final de la auditoria donde se argumente las condiciones en que operará.

Los informes de la auditoría tendrán 2 modelos básicos: El primero de ellos consiste en lo referente a los resultados emitidos durante el proceso de auditoria enfocada a los hallazgos y recomendaciones. El segundo de ellos consiste en el resultado final de la auditoria donde se argumenten las condiciones en que operará el SEI.

Las recomendaciones realizadas deberán ser precisas y objetivas, enfocadas a cumplir la continuidad del SEI. Deberán igualmente incluir los datos, hechos y observaciones en que se basen las recomendaciones propuestas.

Los informes se tipificarán de la siguiente manera:

- Informes Parciales: son los referentes a los resultados emitidos durante el proceso de auditoría, los cuales tendrán **calidad de reservados** en términos de las disposiciones aplicables en materia de transparencia y acceso a la información.

- Informe previo a la jornada: es el correspondiente a los resultados finales de la auditoría previo al día de la jornada. Dicho informe **será público**.

- Informe de la auditoría realizada el día de la jornada: da cuenta del desempeño y disponibilidad del sistema el día de la jornada, así como de los eventos relevantes dentro del SEI durante su funcionamiento.

- Informe de evaluación que considere el cierre de operaciones del SEI, así como la etapa de evaluación del mismo, donde contenga

INSTITUTO ELECTORAL CIUDAD DE MÉXICO

UNAM FES Aragón

los resultados y actividades realizadas, así como las observaciones y/o recomendaciones.

IX. EXCLUSIONES

El desarrollo de las pruebas de seguridad y la revisión de calidad en términos de funcionalidad no incluye:

- Cambios a la infraestructura.
- Implementación de las recomendaciones.

X. CONSIDERACIONES RESPECTO AL ALCANCE.

Los alcances de la presente propuesta podrán modificarse de común acuerdo entre ambas partes; si dichas modificaciones son considerables impactarán en un incremento del costo del proyecto, si se consideran mínimas y dentro de lo razonable no tendrán costo adicional.

XI. APORTACIONES

"EL INSTITUTO" se compromete a aportar a "LA UNAM" la cantidad de $860,000.00 (ochocientos sesenta mil pesos 00/100 M.N.) más IVA, lo cual da un total de $997,600.00 (novecientos noventa y siete mil seiscientos pesos 00/100 M.N.). Dicha cantidad será otorgada por el IECM de la forma siguiente:

MOMENTO EN QUE SE EFECTUARÁ LA APORTACIÓN	MONTO
El 50% a la firma del convenio, a más tardar 5 días hábiles a partir de la suscripción del convenio, contra la entrega del plan de trabajo de **"LA AUDITORÍA"**.	**$498,800.00**
El 50% restante contra la entrega del informe de evaluación de **"LA AUDITORÍA"**, a más tardar 5 días hábiles posteriores a la entrega.	**$498,800.00**
TOTAL	**$997,600.00**

INSTITUTO ELECTORAL
CIUDAD DE MÉXICO

UNAM
FES
Aragón

FORMA DE OTORGAR LA APORTACIÓN. Las aportaciones serán cubiertas en moneda nacional, mediante transferencia electrónica a solicitud por escrito de "LA UNAM" a la cuenta bancaria número 00446634494 del Banco BBVA Bancomer, Clabe 012180004466344942, Sucursal 7684, Plaza 001 Concepción Béistegui, a nombre de la Universidad Nacional Autónoma de México.

"EL INSTITUTO", entregará a "LA UNAM" en un plazo no mayor de 5 días naturales posteriores a la realización de las transferencias realizadas en los momentos establecidos en el Convenio, copia impresa o electrónica del documento comprobatorio.

M. en C. MARCELO PÉREZ MEDEL
Responsable de la auditoria

M. en C. JESÚS HERNÁNDEZ CABRERA
Corresponsable de la auditoría

SEI 2020

06-feb-2020

UNAM FES ARAGON

http://

Encargado del proyecto	
Fechas de inicio y fin del proyecto	25-feb-2020 - 27-mar-2020
Progreso	0%
Tarea	44
Recursos	4

Preliminar, para ajustar fechas

Tarea

Nombre	Fecha de inicio	Fecha de fin
Auditoria 2020 al Sistema Electrónico por Internet del Instituto Electoral de la Ciudad de México.	25/02/20	26/03/20
Reunión de inicio de proyecto *Presentación del plan general de auditoria* *Revisión de las auditorias previas*	25/02/20	25/02/20
1.-Pruebas de caja Negra en términos de funcionalidad al sistema SEI *Previo al primer simulacro*	25/02/20	11/03/20
Diseño y escritura del plan de pruebas de funcionalidad de caja negra. *Lo prepara la UNAM realizara avances previo al Kickoff*	25/02/20	25/02/20
Recopilación de la información del sistema *El instituto proporcionará a la UNAM la documentacion técnica referente a la aplicacion PREP y Prep Casilla (App Movil)*	25/02/20	29/02/20
El IECM Proporcionará la documentación técnica normativa para la implementación y operación del SEI *Con oficio*	25/02/20	29/02/20
Proporcionar a "La UNAM" el diagrama de la arquitectura de la solución de software, documentando todos los nodos y tecnologías involucradas en la misma.	25/02/20	29/02/20
Informar por escrito el proceso de desarrollo de Software, metodologia o marco de trabajo que emplea para el desarrollo de software del SEI	25/02/20	29/02/20
Proporcionar a "La UNAM" Los diagramas de caso de uso (o equivalente) la cual documente el levantamiento de requerimientos de funcionalidades.	25/02/20	29/02/20
Exponer en una reunión presencial o a distancia, la propuesta de solución implementada para el SEI.	25/02/20	29/02/20
Preparación de las pruebas funcionales de caja negra. *(UNAM) Preparacion de los casos de prueba* *(IECM) Preparar las estaciones de trabajo, las bases de datos los datos de prueba solicitados y cuentas de usuario*	1/03/20	2/03/20
Ejecución de las pruebas funcionales de caja negra *En las instalaciones del IECM, de ser posible se hará en un sólo día*	3/03/20	4/03/20
Escritura y entrega del informe preliminar de las pruebas funcionales de caja negra	5/03/20	7/03/20
Atender las recomendaciones del informe preliminar. *Implementa el IECM*	8/03/20	11/03/20
2.- Análisis de vulnerabilidades a la infraestructura tecnológica	28/02/20	26/03/20

Tarea

Nombre	Fecha de inicio	Fecha de fin
Junta de inicio para presentar las actividades y entrega de la lista de activos a analizar	28/02/20	28/02/20
Requerimiento del INE *Este tipo de pruebas son estáticas y no se realiza un "ataque", se verifica que las versiones de las tecnologías no tengan reportadas vulnerabilidades. Es un proceso documental* *Consideramos que la podemos adelantar antes del primer simulacro* *Se debe entregar la lista de los activos que soportan el sistema PREP y Prep casilla. Modelos, Versiones de firmware, Versiones de S.O, Versiones de servicios, incluyendo BD y Servidor de aplicaciones, SLA de los servicios de terceros*		
Revisión de la configuración de seguridad de la infraestructura tecnológica	2/03/20	26/03/20
Diseño y escritura del Plan de revisión de configuraciones de la infraestructura	26/03/20	26/03/20
Ejecución de la revisión de las configuraciones	2/03/20	3/03/20
Escritura del Informe preliminar de la revisión de configuraciones de la infraestructura	4/03/20	5/03/20
Periodo de remediación	6/03/20	10/03/20
Análisis de vulnerabilidades	1/03/20	18/03/20
Diseño y escritura del plan de trabajo detallado para las pruebas de penetración a la infraestructura tecnológica.	1/03/20	2/03/20
Análisis de vulnerabilidades y explotación	5/03/20	8/03/20
(E: Analisis de vulnerabilidades y explotacion (informe preliminar del analisis de vulnerabilidades en la infraestructura, donde indique el detalle de cada hallazgo identificado)		
Periodo de remediación al menos 10 días	9/03/20	18/03/20
Deberá aplicar recomendaciones, por ejemplo: aplicar un parche de S.O., actualizar bibliotecas, actualizar algún firmware, Hardening, etc.		
Pruebas de penetración	1/03/20	13/03/20
Ejecutar pruebas de penetración	1/03/20	1/03/20
Informe preliminar de las pruebas de penetración a la infraestructura tecnológica	3/03/20	3/03/20
Periodo de remediación	10/03/20	12/03/20
Informe de la aplicación de recomendaciones de las pruebas de penetración a la infraestructura tecnológica	13/03/20	13/03/20
Informe final del análisis de vulnerabilidades a la infraestructura tecnológica	14/03/20	16/03/20
3.- Firma del sistema auditado, verificación el 1o de Julio y revisión el 1o de Julio de Bases de datos en Cero	14/03/20	18/03/20
Firma del software para verificar que el sistema auditado es el que se ejecutara el día de la elección. Revisión de bases de datos en 0 el día 0		
Diseño del procedimiento Técnico verificar que los programas auditados son los mismos que se utilizaran el día de la jornada electoral	14/03/20	18/03/20
Diseño y escritura del diagrama de flujo del procedimiento	14/03/20	18/03/20

Tarea

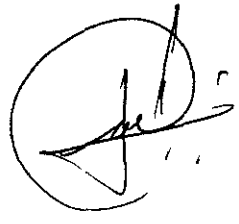
Nombre	Fecha de inicio	Fecha de fin
Generación, obtención y validación de huellas criptográficas del sistema auditado e instalado *fechas establecidas en última reunión*	14/03/20	16/03/20
Generación, obtención y validación de huellas criptográficas en SHA-256 del sistema que operará el día de la jornada electoral	14/03/20	14/03/20
Validación de la información inicial y final de la base de datos	14/03/20	14/03/20
Escritura y entrega de la Constancia de hechos de la verificación del sistema y bases de datos en cero	14/03/20	15/03/20
4.- Pruebas de negación de servicio	3/03/20	10/03/20
Diseño y Escritura del Plan de ataques de denegación de servicio DoS.	3/03/20	3/03/20
Preparación de las pruebas DoS	4/03/20	5/03/20
Ejecutar Pruebas DoS	6/03/20	6/03/20
Informe de resultados que incluyen las estádisticas del tráfico generado.	9/03/20	10/03/20
Informe de Evaluación de la auditoria.	20/03/20	24/03/20

Recursos

Nombre	Función
Probador de Software	Diseña estrategias especificas para la realización de pruebas funcionales de caja negra, de acuerdo con los criterios de auditoria establecidos para el proyecto. Define escenarios y casos de prueba. Elabora y organiza datos de prueba conforme a los escenarios definidos. Establece los requerimientos del ambiente necesario para la realización de las pruebas. Selecciona y habilita herramientas informáticas de apoyo para las pruebas funcionales. Verifica la funcionalidad de los programas de software acorde a los criterios de auditoria definidos. Identifica y documenta los hallazgos: verifica que hayan sido subsanadas a través de nuevas pruebas
Pentester	Identifica las técnicas a utilizar para la realización de pruebas de acuerdo a las caracteristicas de la infraestructura de TI. Configura y ejecuta herramientas de Pentest. Identifica potenciales vulnerabilidades en la infraestructura. Analiza la información sobre potenciales vulnerabilidades para definir técnicas y estrategias de explotación. Documenta hallazgos de vulnerabilidades. Clasifica hallazgos de acuerdo con metodologías como CVSS. Elabora informes de las pruebas de penetración.
Responsable Técnico	Identifica las técnicas a utilizar para la realización de pruebas de acuerdo a las caracteristicas de la infraestructura de TI. Configura y ejecuta herramientas de Pentest. Identifica potenciales vulnerabilidades en la infraestructura. Analiza la información sobre potenciales vulnerabilidades para definir técnicas y estrategias de explotación. Documenta hallazgos de vulnerabilidades. Clasifica hallazgos de acuerdo con metodologías como CVSS. Elabora informes de las pruebas de penetración.

Recursos

Nombre	Función
Líder Técnico	Especialista técnico encargado de detallar la planeación de la línea de trabajo en tareas específicas para cada uno de los integrantes de su equipo. Implementa las metodologías y herramientas tecnológicas específicas para la realización de la línea de trabajo. Orienta y supervisa a los grupos de trabajo específicos para la realización de actividades técnicas. Integra y verifica la calidad técnica de los entregables parciales y finales de la línea de trabajo. Resuelve los asuntos técnicos o bien los escala oportunamente. Genera reportes sobre el avance, oportunidades y riesgos técnicos.



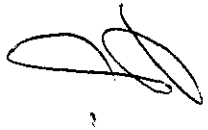
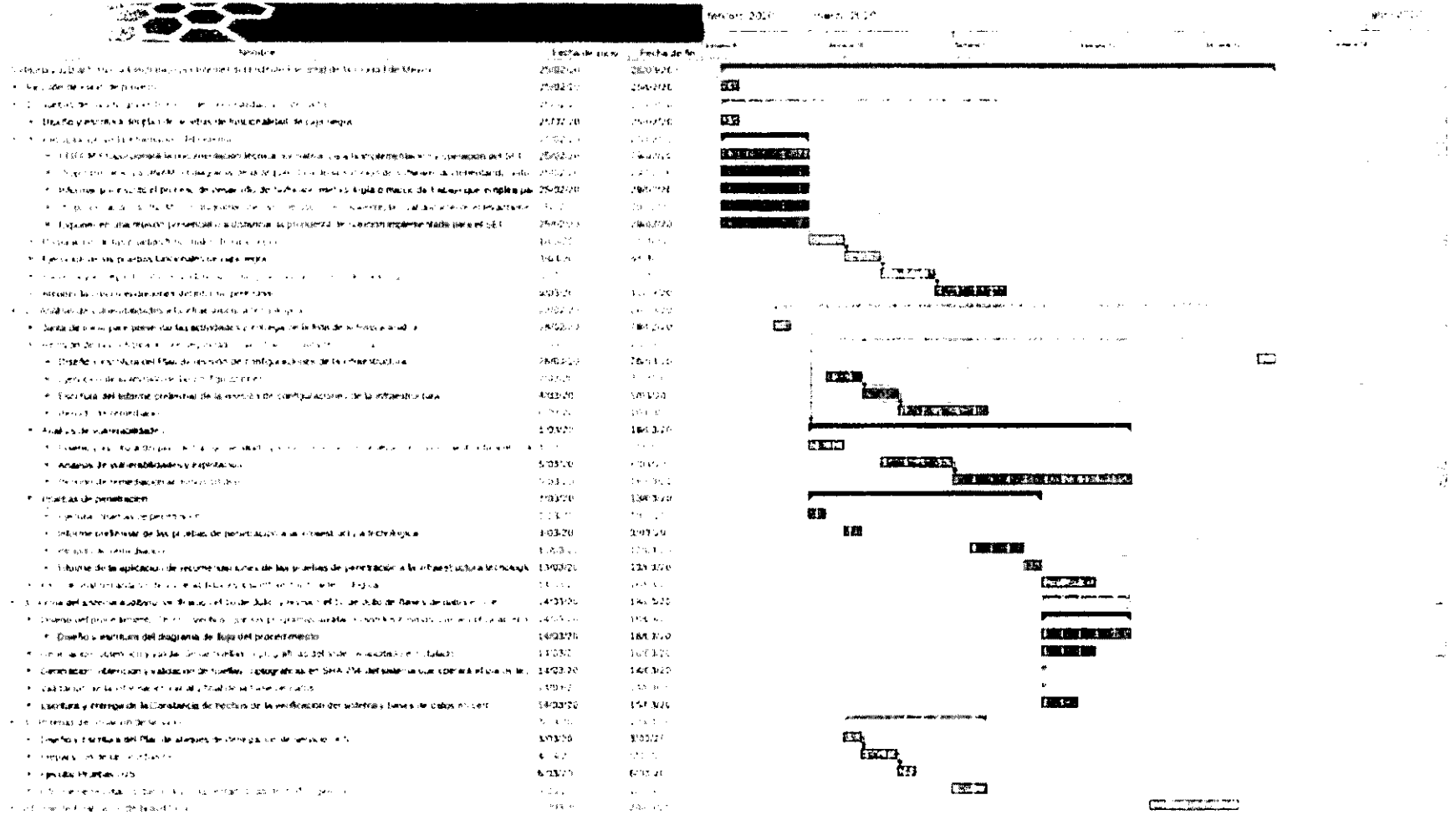


Diagrama de Gantt



FACULTAD DE ESTUDIOS
SUPERIORES ARAGÓN

CENTRO TECNOLÓGICO ARAGON

Síntesis Curricular del Centro Tecnológico de la Facultad de Estudios Superiores Aragón de la Universidad Nacional Autónoma de México

La Facultad de Estudios Superiores Aragón de la Universidad Nacional Autónoma de México (FES-UNAM)es una Institución de Educación Superior dedicada a la formación de profesionistas de excelencia, mediante actividades que aportan valor en cada una de las áreas de las distintas carreras que en ella se imparten, con la firma convicción en el uso de las tecnologías a favor del proceso de enseñanza – aprendizaje, dando oportunidad para el desarrollo de los académicos y trabajadores mediante la capacitación constante, estabilidad y el reconocimiento a sus labores. Apegándose al marco institucional, al uso racional de nuestros recursos, a la calidad en el servicio y anteponiendo siempre el beneficio de la sociedad.

La FES Aragón tiene 41 años de existencia, trabajando siempre bajo los tres principales objetivos de la UNAM, impartir educación, realizar investigación y difundir la cultura. Como parte de la Facultad se encuentra en Centro Tecnológico Aragón, el cual desde hace 21 años desarrolla proyectos de vinculación con entidades de gobierno, empresas y otras universidades, entre los múltiples proyectos en los que ha participado, destacan en el ámbito electoral, la creación de un prototipo de urna electrónica en 2003 para el entonces IEDF y más recientemente:

"Auditoría Informática al Programa de Resultados Electorales Preliminares PREP y Conteos Rápidos 2015"

Numero de convenio: No. 41773-1483-16-VI-15

"Auditoria Informatica al Programa de Resultados Electorales Preliminares PREP y Conteos Rapidos 2016" para el Organismo Publico Local Electoral del Estado de Veracruz

Numero de convenio: No. 44910-1180-17-V-16

"Auditoria Informatica al Programa de Resultados Electorales Preliminares PREP 2017" para el Instituto Electoral del Estado de Mexico

Número de convenio. No. 47780-596-2-III-17

"Auditoria de verificacion y análisis del sistema electrónico por Internet" para el Instituto Electoral de la Ciudad de México.

Número de convenio. No. 48853-1669-22-VI-17

El Centro Tecnológico Aragón cuenta con personal con experiencia en desarrollo y evaluación de Tecnologías de la Información. Y con certificaciones tales como:

- Certificación en metodología de desarrollo de Software, Scrum Master. Certificant ID: 000431528. https://www.scrumalliance.org/ 2015 - 2018
- Certificación de Desarrollador SCRUM, CSD, Certificacion en Scrum Developer. Certificant ID: 431528. https://www.scrumalliance.org/ 2016 - 2018
- Certificación en auditor en sistemas de Software y Seguridad, CISA, Certified Information Systems Auditor. Centification number: 17141684

Anexo al presente se envían primer y última hoja de cada uno de los convenios antes mencionados.

Adicionalmente participamos en las auditorias del PREP 2018 para la Ciudad de México, Estado de Veracruz y Estado de México. anexamos los informes finales.

REGISTRO UNAM: 41773-1483-16-VI-15

CONVENIO ESPECÍFICO DE COLABORACIÓN QUE CELEBRAN POR UNA PARTE, LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, EN LO SUCESIVO "LA UNAM", REPRESENTADA EN ESTE ACTO POR EL DR. EDUARDO BÁRZANA GARCÍA, EN SU CARÁCTER DE SECRETARIO GENERAL, ASISTIDO POR EL M. EN I. GILBERTO GARCÍA SANTAMARÍA GONZÁLEZ, DIRECTOR DE LA FACULTAD DE ESTUDIOS SUPERIORES ARAGÓN; Y POR LA OTRA PARTE, EL INSTITUTO ELECTORAL DEL DISTRITO FEDERAL, "EL IEDF", REPRESENTADO EN ESTE ACTO POR EL MTRO. MARIO VELÁZQUEZ MIRANDA, CONSEJERO PRESIDENTE DEL CONSEJO GENERAL, Y EL LIC. RUBÉN GERALDO VENEGAS, SECRETARIO EJECUTIVO Y REPRESENTANTE LEGAL, CON LA ASISTENCIA DEL LIC. ALEJANDRO FIDENCIO GONZÁLEZ HERNÁNDEZ, SECRETARIO ADMINISTRATIVO, A QUIENES EN CONJUNTO SE DENOMINARÁN "LAS PARTES", CONFORME A LOS ANTECEDENTES, DECLARACIONES Y CLÁUSULAS SIGUIENTES:

A N T E C E D E N T E S

1. El 22 de agosto de 2001, **"LAS PARTES"**, celebraron un Convenio General de Colaboración Académica Científica y Cultural, con número de registro **41773-1483-16-VI-15**, cuyo objeto, conforme a la cláusula Primera, consiste en establecer las bases para organizar y desarrollar actividades en los campos de docencia, investigación y difusión de la cultura. Asimismo, en la cláusula Segunda, inciso c), se estipuló promover la organización de cursos, talleres y seminarios en áreas de interés para ambas.

2. En la cláusula Tercera del referido Convenio, **"LAS PARTES"** acordaron que para la ejecución de las acciones referidas en el mismo, celebrarían Convenios Específicos de Colaboración, en los cuales se detallaría con toda precisión la realización de las actividades que se pretendan llevar a cabo en forma concreta.

3. En la cláusula Novena del citado Convenio, **"LAS PARTES"** establecieron que dicho instrumento tendría una vigencia indefinida, iniciando a partir de la fecha de su suscripción.

D E C L A R A C I O N E S

REGISTRO UNAM: 48853-1669-22-VI-17

CONVENIO ESPECIFICO DE COLABORACIÓN PARA LA AUDITORÍA DE VERIFICACIÓN Y ANÁLISIS DEL SISTEMA ELECTRÓNICO POR INTERNET, EN LO SUCESIVO EL "SEI", QUE CELEBRAN POR UNA PARTE, LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, EN LO SUCESIVO LA "UNAM". REPRESENTADA EN ESTE ACTO POR EL DR. LEONARDO LOMELÍ VANEGAS, EN SU CARÁCTER DE SECRETARIO GENERAL, ASISTIDO POR EL M. EN I. FERNANDO MACEDO CHAGOLLA, DIRECTOR DE LA FACULTAD DE ESTUDIOS SUPERIORES ARAGÓN; Y POR LA OTRA PARTE, EL INSTITUTO ELECTORAL DEL DISTRITO FEDERAL, EN LO SUCESIVO EL "IEDF", REPRESENTADO EN ESTE ACTO POR EL MTRO MARIO VELÁZQUEZ MIRANDA, CONSEJERO PRESIDENTE DEL CONSEJO GENERAL, EL LIC. RUBÉN GERALDO VENEGAS, SECRETARIO EJECUTIVO Y REPRESENTANTE LEGAL, CON LA INTERVENCIÓN DEL MTRO ALEJANDRO FIDENCIO GONZÁLEZ HERNÁNDEZ, SECRETARIO ADMINISTRATIVO; A QUIENES EN CONJUNTO SE DENOMINARÁ LAS "PARTES", CONFORME A LOS ANTECEDENTES, DECLARACIONES Y CLÁUSULAS SIGUIENTES:

A N T E C E D E N T E S

1. El 9 de octubre del año 2015, las "**PARTES**" celebraron un Convenio General de Colaboración Académica, Científica y Cultural, con el siguiente número de registro **42227-1937-12-VIII-15** cuyo objeto conforme a su cláusula Primera, consiste en organizar y desarrollar actividades en los campos de la docencia, la investigación y difusión de la cultura en materia político – electoral. Asimismo en la cláusula Segunda, inciso g), se estableció favorecer la creación de esquemas de investigación y cooperación para el fortalecimiento de los mecanismos de participación ciudadana señalados en la Ley de Participación Ciudadana del Distrito Federal

2. En la cláusula Tercera del Convenio anteriormente referido, las "**PARTES**" establecieron la posibilidad de celebrar Convenios Específicos en los que se detallarían los respectivos compromisos para la consecución del objeto del Convenio General, mismos que deberían ser acordados previamente entre las "**PARTES**"

3. Conforme a lo dispuesto en la cláusula Sexta del referido Convenio General, se estableció que su vigencia sería indefinida

REGISTRO UNAM: 44910-1180-17-V-16

CONVENIO ESPECÍFICO DE COLABORACIÓN QUE CELEBRAN POR UNA PARTE, LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO, EN LO SUCESIVO "LA UNAM", REPRESENTADA EN ESTE ACTO POR EL DR. LEONARDO LOMELÍ VANEGAS, EN SU CARÁCTER DE SECRETARIO GENERAL, ASISTIDO POR EL M. EN I. GILBERTO GARCÍA SANTAMARÍA GONZÁLEZ, DIRECTOR DE LA FACULTAD DE ESTUDIOS SUPERIORES ARAGÓN; Y POR LA OTRA PARTE, EL ORGANISMO PÚBLICO LOCAL ELECTORAL DE VERACRUZ, EN LO SUCESIVO "EL OPLE", REPRESENTADO EN ESTE ACTO POR EL LIC. JOSÉ ALEJANDRO BONILLA BONILLA, CONSEJERO PRESIDENTE DEL CONSEJO GENERAL, Y EL MTRO. HUGO ENRIQUE CASTRO BERNABE, SECRETARIO EJECUTIVO Y REPRESENTANTE LEGAL, CON LA ASISTENCIA DE LA DRA. ZAIDÉ ZAMUDIO CORRO, SECRETARIA ADMINISTRATIVA, A QUIENES EN CONJUNTO SE DENOMINARÁN "LAS PARTES", CONFORME A LOS ANTECEDENTES, DECLARACIONES Y CLÁUSULAS SIGUIENTES:

A N T E C E D E N T E S

1. El 10 de febrero de 2014, se publicó en el Diario Oficial de la Federación, el Decreto por el que se reforman, adicionan y derogan diversas disposiciones de la Constitución Política de los Estados Unidos Mexicanos, en específico en materia político-electoral, destacando la creación del Instituto Nacional Electoral, en adelante "EL INE", y de los organismos públicos locales, en adelante "LOS OPLE".

2. El 23 de mayo del año 2014, fue publicado en el Diario Oficial de la Federación el Decreto por el que se expide la Ley General de Instituciones y Procedimientos Electorales, la Ley General de Partidos Políticos, así como se reforman y adicionan diversas disposiciones de la Ley General del Sistema de Medios de Impugnación en Materia Electoral, de la Ley Orgánica del Poder Judicial de la Federación y de la Ley Federal de Responsabilidades Administrativas de los Servidores Públicos, previéndose la obligación de "LOS OPLE" de atender las disposiciones contenidas en los dispositivos legales que le obligan, en concreto por lo que hace a las primeras de las leyes mencionadas.

3. El 09 de noviembre de 2015, en sesión de instalación del Consejo General de "EL OPLE", se dio inicio formal del proceso electoral ordinario local

EDUCACIÓN

Centro de Investigación en Computación

Asunto:

Dr. Oscar Alejandro Rodríguez Paz
Titular de la Unidad de Servicios Informáticos
PRESENTE

ATENTAMENTE
"La Técnica al Servicio de la Patria"

Dr. Marco A. Ramírez Salinas
Director

DIRECCIÓN

c.c.p. Mtro. Mario Velazquez Miranda
Mtra. Myriam Maryon Reyes
Mtra. Carolina del Angel Cruz
Mtra. Gabriela Williams Salazar
Lic. Ruben Gerardo Venegas
Mtro. Alejandro Ulises Gonzalez Hernandez
Lic. Cecilia A. Hernandez Cruz

2020

Folio 113

UNIVERSIDAD NACIONAL AUTÓNOMA DE MEXICO
SECRETARÍA DE DESARROLLO INSTITUCIONAL
Dirección General de Cómputo y de
Tecnologías de Información y Comunicación

DGTIC

Oficio No. TIC/DCV/005/2020

Asunto: Respuesta a oficio IECM/UTSI/036/2020

LIC. OSCAR ALEJANDRO RODRÍGUEZ PAZ
TITULAR DE LA UNIDAD TÉCNICA DE SERVICIOS INFORMÁTICOS
INSTITUTO ELECTORAL DE LA CIUDAD DE MÉXICO (IECM)
P R E S E N T E

Por instrucciones de la Mtra. Ma. De Lourdes Velázquez Pastrana, Encargada del Despacho de la Dirección General de Cómputo y de Tecnologías de Información y Comunicacion (DGTIC), y en respuesta a su oficio IECM/UTSI/036/2020 con fecha del 04 de febrero de 2020, por medio del cual extiende una cordial invitación para que DGTIC-UNAM participe en las actividades relativas a la selección de Auditores Externos para los Servicios de Auditoría al Sistema Informático y a la Infraestructura Tecnológica del Sistema Electrónico por Internet (SEI 2020), le comento lo siguiente:

DGTIC forma parte de las dependencias de la administración central que apoyan a la Rectoria en la planeación y ejecución de proyectos institucionales, por lo que tras la designación del Señor Rector para un segundo periodo, nos encontramos en proceso de análisis de nuestros servicios y de definición de planes de trabajo para los años 2020-2023. Si bien la temática de la invitación que el IECM ha extendido a la DGTIC es de interés para esta Dirección General, en conocimiento de que la Facultad de Estudios Superiores Aragón ha recibido una invitación similar, consideramos oportuno manifestar que, en el supuesto de que la UNAM decidiera presentar la propuesta solicitada, lo realizaría a través de esa entidad académica.

Agradeciendo la gentileza de considerarnos para colaborar con ustedes, sin otro particular, hago propicia la ocasión para enviarle un cordial saludo.

A T E N T A M E N T E
"POR MI RAZA HABLARÁ EL ESPÍRITU"
Cd. Universitaria, Cd. Mx, 06 de febrero de 2020.

DRA. MARCELA PEÑALOZA BÁEZ
DIRECTORA DE COLABORACIÓN Y VINCULACIÓN

INSTITUTO ELECTORAL CIUDAD DE MÉXICO | UNIDAD TÉCNICA DE SERVICIOS INFORMÁTICOS

06 Feb 2020
RECIBIDO

c.c.p. M. en C. María de Lourdes Velázquez Pastrana, Encargada del Despacho de la Dirección General de Cómputo y Tecnologías de Información y Comunicación, UNAM
Lic. Cecilia A. Hernández Cruz, Titular de la Unidad Técnica de Vinculación con Organismos Externos del IECM

MFB/RFMF

EVALUACIÓN TÉCNICA

De conformidad con el Articulo 48 los Lineamientos Generales del Sistema Electrónico por Internet del Instituto Electoral de la Ciudad de Mexico, que a la letra dice: *"En caso de que el Consejo General determine que esta modalidad de emisión del sufragio tenga carácter vinculante para un Proceso Electoral o para Mecanismos e Instrumentos de Participación Ciudadana, previa realización de las pruebas públicas correspondientes, el Instituto Electoral podrá someter al Sistema a una auditoria pública en cada una de sus etapas de desarrollo e implementación, a través de instituciones o empresas con prestigio internacional. Lo anterior se hará en acompañamiento de partidos politicos, candidaturas sin partido y, en su caso, observadores de la Sociedad Civil."*

La Unidad Técnica de Servicios Informáticos realizó una invitación a diversas Instituciones Académicas de la Ciudad de México, para participar en el proceso de selección de auditores externos para el SEI.

En este sentido, y con base en la propuesta técnica enviada por el "Centro Tecnológico Aragón" de la Facultad de Estudios Superiores Aragón de la Universidad Nacional Autónoma de México, a través del Oficio FESAR/CTA/025/2020, la Unidad Técnica de Servicios Informáticos determina que:

El "Centro Tecnológico Aragón" de la Facultad de Estudios Superiores Aragón de la Universidad Nacional Autónoma de México **CUMPLE**, con el total de las especificaciones solicitadas, de acuerdo con lo siguiente:

- Cumple con los apartados de Planeación, Metodología y Revisión, descritos en el artículo 49 de los Lineamientos del SEI.
- Cumple con respecto a la presentación de informes parciales y dictamen final del proceso de auditoria, contemplado en el artículo 52 de los Lineamientos del SEI.

Se agrega como anexo a la presente, el detalle de la Evaluación Técnica del cumplimiento de la Propuesta Técnico - Económica para la auditoría del SEI.

Se emite la presente Evaluación Técnica el 10 de febrero de 2020, para dar continuidad con el proceso de convenio.

Elaboró

Ing. Luis Fernando Pech Salvador
Jefe de Departamento de Web, Seguridad y Nuevas Tecnologías

Revisó

Mtro. Ilse Zahuaicóyotl Flores Rodríguez
Dirección de Infraestructura Informática

Autorizó

Lic. Oscar Alejandro Rodríguez Paz
Titular de la Unidad Técnica de Servicios Informáticos

PROPUESTA TÉCNICA	FES-Aragón
ANEXO TÉCNICO PARA LA CONTRATACIÓN DE LOS SERVICIOS DE AUDITORIA AL SISTEMA INFORMÁTICO Y A LA INFRAESTRUCTURA TECNOLÓGICA DEL SISTEMA ELECTRÓNICO POR INTERNET (SEI 2020) En el marco de las actividades para la implementación y operación del Sistema Electrónico por Internet (SEI 2020) para la Elección de Comisiones de Participación Comunitaria 2020 y la Consulta de Presupuesto Participativo 2020 - 2021, el Instituto Electoral de la Ciudad de México (IECM) requiere que se lleve a cabo una auditoría al sistema informático y a la infraestructura tecnológica que soporta el SEI 2020. **OBJETIVO GENERAL** Realizar una auditoría informática al SEI 2020, con la finalidad de evaluar la integridad en el procesamiento de la información y la generación de los resultados. **ALCANCES** 1. Realizar una auditoría al sistema informático y la infraestructura tecnológica del SEI 2020, se deberán revisar conforme a lo siguiente: a) Funcionalidad de la infraestructura tecnológica del SEI 2020. b) Pruebas funcionales al sistema informático del SEI 2020. c) Pruebas de penetración (Pentest). d) Análisis de vulnerabilidades. e) Pruebas de denegación de servicio. f) Validación de reporte de hallazgos. g) Revisión de la documentación y configuraciones. **CONSIDERACIONES** 1. La auditoría se realizará cuando el SEI 2020 alcance el 100% de avance en su desarrollo. 2. Los alcances podrán modificarse siempre y cuando el IECM y el Auditor estén de acuerdo y manifiesten su consentimiento por escrito. 3. Durante los simulacros que se efectúen en las fechas acordadas, se solicitará el acompañamiento del Auditor en las pruebas que se realizarán. 4. Se realizará una junta de inicio, donde se convocará al personal involucrado en la realización de la auditoría con el objetivo de presentar las actividades consideradas como parte de la auditoría, definir los roles y responsabilidades de las partes, establecer las metodologías y estándares con las que se realizará la auditoría, así como los tiempos generales de ejecución. Se expondrán plan de trabajo y se acordarán las formas de dar seguimiento al proceso de auditoría. 5. Se realizará un informe parcial sobre los hallazgos encontrados y se enviarán por escrito a la Unidad Técnica de Servicios Informáticos (UTSI), así como las recomendaciones necesarias para su remediación; posterior a ello, la UTSI realizará las mitigaciones respectivas, al finalizar estas, el Auditor realizará nuevamente las revisiones; dicho proceso se ejecutará hasta completar todos los hallazgos encontrados. 6. Se realizará un informe final de todas las actividades realizadas con sus reactivas evidencias excluyendo el informe parcial, considerado los siguiente: a) Resumen ejecutivo. b) Resultado de las pruebas. c) Recomendaciones generales. **Elaboración de propuesta técnico – económica**	Cumple

PROPUESTA TÉCNICA	FES-Aragón

El ente Auditor deberá estructurar la propuesta técnico-económica de la siguiente manera:

1. Propuesta técnica, considerando los rubros del presente documento.
2. Plan de trabajo detallando.
3. Protocolos y metodologías de trabajo para llevar a cabo las actividades
4. Currículum de la Institución o Universidad.
5. Lista del personal que realizará la auditoria, detallando certificaciones y grados académicos (presentar copia simple de la documentación que acredite dichos estudios).
6. Presentar ejemplos comprobables de informes relacionados con los resultados obtenidos en proyectos similares que haya realizado
7. Presentar ejemplos de esquemas de validación de software, ejecutados en proyectos similares llevados a cabo anteriormente.
8. Propuesta económica incluyendo los impuestos respectivos.

REQUERIMIENTOS DE AUDITORÍA

i. Funcionalidad de la Infraestructura tecnológica del SEI 2020

La revisión se realizará únicamente a los elementos de infraestructura que intervienen en el flujo de operación del SEI 2020. La revisión de la infraestructura deberá considerar, al menos, los siguientes aspectos:

1. Verificar el grado de disponibilidad de la infraestructura de cómputo que soporta al sistema informático.
2. Comprobar que la arquitectura de la infraestructura de cómputo y comunicaciones corresponda a la necesidad del sistema informático.
3. Verificar que la base datos del SEI se encuentre alojada en un Centro de Cómputo propiedad del Instituto.
4. Comprobar que el Centro de Cómputo (Data Center) cuente con las condiciones mínimas de operación.
5. Verificar que el servicio de internet esté soportado por dos ISP diferentes
6. Verificar que la base de datos se encuentre en alta disponibilidad.
7. Verificar que los servidores de aplicación estén balanceados
8. Verificar que las instancias de bases de datos del sistema se encuentren ligadas a las aplicaciones
9. Revisar que cuente con las actualizaciones y parches necesarios.
10. Revisar que existan mecanismos y rutinas de seguridad.
11. Verificar que, en los servidores, únicamente estén activos los servicios y puertos necesarios para la correcta operación del sistema.
12. Verificar que los niveles de seguridad de los usuarios respondan únicamente a las actividades para los cuales fueron creadas.
13. Verificar el rendimiento y la capacidad de procesamiento de las máquinas virtuales.
14. Revisar los controles de seguridad y datos
15. Realizar análisis de vulnerabilidades.
16. Verificar que no existan "Buffers Overflow".
17. Revisar de la administración de sesiones
    a. Los niveles de autorizaciones y privilegios
    b. El manejo de errores.
18. Verificar que los sistemas informáticos que formen parte del SEI 2020 contengan los niveles de seguridad adecuados para la integridad de los datos.
19. Revisar que los servidores y aplicaciones cuenten con los parches necesarios.
20. Verificar la existencia de bitácoras del sistema, y que puedan ser auditables en caso de impugnaciones.
21. Verificar que las comunicaciones se ejecuten en un canal de comunicación seguro.

PROPUESTA TÉCNICA	FES-Aragón
Las pruebas se realizarán utilizando las metodologías propuestas. Se analizará la seguridad de la red desde el punto de vista externo (Internet) desde la red local del Instituto (LAN); desde una línea de suscriptor digital asimétrico (ADSL), servicios de movilidad E, GPRS, 3G, y 4G, y mediante la utilización de enlaces privados del Instituto; todas ellas sin el conocimiento previo de la topología de red. Se realizarán estas pruebas con la intención de mostrar el grado de exposición de las aplicaciones, bases de datos e infraestructura del Instituto, las pruebas incluirán: 1. Pruebas de "caja negra" y "caja blanca". 2. Pruebas de "man in the middle". 3. Pruebas a las instancias de base de datos. 4. Pruebas de penetración al sistema operativo. 5. Pruebas de Injection. 6. Pruebas de penetración hacia los aplicativos. En esta etapa se depositará una bandera en los objetivos que haya sido posible acceder, sin afectar la operación y sin modificar la información alcanzada. **iv. Análisis de vulnerabilidades** Para realizar el análisis de vulnerabilidades en la infraestructura tecnológica del SEI, se contemplará lo siguiente: 1. Ejecución de herramientas automatizadas de búsqueda de vulnerabilidades. 2. Pruebas de inyección de código malicioso. 3 Pruebas de penetración internas y externas que incluirán pruebas de acceso a los diversos recursos del sistema informático. 4. Análisis de código estático que consistirán en técnicas de análisis de código fuente. 5. Pruebas de código dinámico sobre la aplicación en ejecución. 6. Escaneo de puertos - identificando así los sockets del SEI 2020; los cuales deberán ser exclusivamente los necesarios para atender los servicios solicitados. Pruebas de vulnerabilidad: se evidenciará y documentará el grado de visibilidad y el nivel de exposición ante ciertos riesgos de inclusión de código malicioso, o algún otro ataque controlado; comprobando así la efectividad de la prueba. Esto es, que para considerar que una vulnerabilidad fue exitosa es necesario contar con la bandera o evidencia de intrusión. Se realizarán pruebas tanto automatizadas como manuales para obtener acceso a todos los recursos de información de los dispositivos localizados como objetivo en la etapa anterior: 1. Identificar riesgos utilizando herramientas de libre uso o propietarias. 2. Identificar riesgos en sistemas operativos y en bases de datos. 3. Identificar "exploits" de acuerdo con las vulnerabilidades encontradas. Los tipos de vulnerabilidades que se intentarán explotar en el aplicativo serán: 1. SQL Injection. 2. Cross Site Scripting. 3. Errores en las aplicaciones. 4. Errores en los patrones de base de datos 5. Directorios ocultos. 6. LDAP Injection. 7. Command Injection. 8. Buffer overflow. 9. Manipulación de parámetros http. 10. Corrupción de archivos. 11. Envenenamiento de Cookies. **v. Pruebas de denegación de servicio** Las pruebas de negación de servicio deberán considerar dos apartados:	

PROPUESTA TÉCNICA	FES-Aragón

ii. Pruebas funcionales al sistema informático del SEI 2020.

Las pruebas se deberán realizar en términos de la funcionalidad del sistema informático del SEI 2020, y deberá considerar, al menos, los siguientes aspectos:

1. Se debe analizar el funcionamiento de la aplicación con relación a la Guía para la implementación del Sistemas Electrónico por Internet en su fase de operación
2. Se debe verificar el cumplimiento de las especificaciones funcionales y requerimientos contenidos en la documentación técnica y normatividad aplicable que será proporcionada por el IECM.
3. Validar que el sistema informático del SEI 2020 que operará los días de consulta y elección, corresponda al software auditado, así como que la base de datos se encuentre sin registros adicionales a los necesarios para que el sistema opere. La validación respecto a la correspondencia del software auditado y el utilizado en la operación, se tendrá que realizar al inicio, durante y al final de la operación del sistema informático del SEI 2020.
4. Revisar que exista un control de versiones del SEI 2020
5. El Auditor deberá llevar a cabo un procedimiento técnico para verificar que los programas auditados se encuentren operando desde el inicio y hasta el cierre de operación del sistema informático, así como que la base de datos se encuentre debidamente inicializada. Dicho procedimiento deberá ser validado por el personal que el Instituto designe para tal efecto contemplando los siguientes aspectos como mínimo:
    a) Generación, obtención y validación de huellas criptográficas en SHA-256 del software SEI 2020 auditado
    b) Generación, obtención y validación de huellas criptográficas en SHA-256 del software SEI 2020 instalado en el ambiente productivo que estará en operación los días de consultas y elección.
    c) Validación de la información inicial y final de la base de datos del SEI 2020

iii. Pruebas de penetración (Pentest)

Las pruebas de penetración se llevarán a cabo tanto, desde el interior como desde el exterior de la red de datos a examinar y deberán enfocarse en: servidores, aplicaciones y equipos de comunicaciones.

Para la realización de las pruebas de **Pentest**, el Auditor deberá identificar los puntos de acceso y consulta que tiene el Instituto para el público en general, con la finalidad de ubicar la infraestructura que lo soporta. En este proceso podrá hacer uso de herramientas de mapeo e identificación de red, estableciendo los límites de la infraestructura de comunicaciones para desarrollar un modelo para las siguientes etapas:
Reconocimiento de la red externa:

1. Identificación de puntos con presencia en Internet.
2. Obtención de registros públicos (NIC).
3. Enumeración de nodos externos.
4. Enumeración de servicios externos.
5. Enumeración de manejadores de base de datos
6. Análisis del contexto general del Instituto.

Basados en los resultados de la etapa anterior se enumerará y conocerán los nodos y servicios activos, así como los que se encuentran en modalidad silenciosa. A partir de esta información, se elaborará un diagrama que registre sistemas operativos, aplicaciones operativas y dispositivos de red alcanzables.

1. Documentación de los nodos activos.
2. Documentación de los nodos ocultos.
3. Enumeración de los nodos confiables.
4. Determinar los tipos de sistemas operativos
5. Determinar la configuración de los sistemas operativos.
6. Determinar los tipos de manejadores de bases de datos.

PROPUESTA TÉCNICA	FES-Aragón
1. Tráfico no malintencionado que consiste en transacciones sintéticas que simulen el tráfico legítimo que se espera el día de la jornada. 2. Tráfico de red malintencionado, consistente en paquetes de red malformados. Los ataques de denegación de servicio deben contemplar, al menos, tráfico de red malintencionado con las siguientes características: 1. Ataques volumétricos por protocolo TCP. a. Al menos de 400 Mbps de throughput. b. Al menos realizar SYN FLOOD. 2. Ataques volumétricos por protocolo UDP. a. Al menos de 400 Mbps de throughput. b. Al menos realizar DNS AMPLIFICATION. 3. Ataques volumétricos por protocolo ICMP. a. Al menos de 400 Mbps de throughput. b. Al menos realizar ICMP FLOOD. 4. Ataques en la capa de aplicación (HTTP). a. Al menos realizar SLOWRIS ATACK. Las pruebas mencionadas anteriormente deberán realizarse de manera concurrente; considerando la generación de tráfico malintencionado (SYN FLOOD, DNS AMPLIFICATION, ICMP FLOOD, SLOWRIS ATACK) en un volumen que represente las condiciones de un ataque. Durante las pruebas, cada simulación de ataque deberá apegarse a las condiciones de un ataque para hacer que el SEI 2020 quede fuera de línea (no disponible) por, al menos 2 minutos, previo a que el IECM efectué la contramedida para la mitigación. Realizar ataques de denegación de servicio que permitan identificar, evaluar y aplicar las medidas necesarias para asegurar la correcta y continua disponibilidad del servicio Web del SEI 2020, durante su periodo de operación. Documentar los hallazgos detectados durante la realización de las pruebas de negación de servicio. **vi. Validación de reporte de hallazgos:** El Instituto presentará al Auditor la retroalimentación acerca de los hallazgos encontrados con el fin de descartar falsos positivos (hallazgos que indican incorrectamente sobre la presencia de una vulnerabilidad) y homologar criterios de interpretación de dichos hallazgos. Una vez validados los hallazgos, el IECM aplicará los diferentes controles necesarios para mitigarlos y atenderlos en su caso. El Auditor deberá realizar una revisión final, para validar que el Instituto haya aplicado los controles necesarios para atender los hallazgos reportados y constatar que las remediaciones fueron aplicadas y mitigadas al 100%. El Auditor, durante el tiempo de los servicios deberá asesorar y acompañar al personal de la UTSI, a fin de atender y aplicar las observaciones y/o recomendaciones, que en su caso procedan respecto de la revisión, con la finalidad de mitigar los riesgos que se detecten. Evidenciar las vulnerabilidades en aplicaciones, base de datos e infraestructura que permitan acceso o negación de los servicios. Consideraciones de la valoración de vulnerabilidades. El informe de los hallazgos encontrados deberá contener: 1. Riesgos de seguridad. 2. URLs escaneadas. 3. URLs vulnerables. 4. Causas de los problemas de seguridad clasificados por tipo de amenaza. 5. Tareas necesarias para la mitigación de los problemas de seguridad encontrados. 6. En caso de obtener acceso a algún servidor de bases de datos o servidor interno, se enumerarán los manejadores de bases de datos que se pueden "ver", el punto desde donde se tuvo acceso y se intentó comprometerlos. Toda la información e la que se tenga acceso, o	

PROPUESTA TÉCNICA	FES-Aragón
bien, se obtenga a partir de los resultados de la prueba. (Depositar banderas en los objetivos que haya sido posible acceder, sin afectar la operación y sin modificar la información alcanzada) Identificar debilidades de seguridad en la infraestructura tecnológica mediante la ejecución de pruebas de penetración y revisión de configuraciones de seguridad Clasificar el impacto y documentar las vulnerabilidades identificadas con el propósito de recomendar al IECM las posibles medidas para la mitigación de las vulnerabilidades que previamente fueron identificadas y documentadas. Verificar que las medidas implementadas por el IECM hayan atendido adecuadamente las vulnerabilidades reportadas. **vii. Revisión de la documentación y configuraciones.** Analizar las configuraciones de los dispositivos que conforman la infraestructura tecnológica con base en mejores prácticas de seguridad informática para identificar oportunidades y emitir recomendaciones orientadas al fortalecimiento de esta. Comprobar que se cuente con la siguiente documentación técnica del sistema: 1 Diagramas de flujo de la funcionalidad del sistema 2 Manuales de operación del sistema 3 Diagrama entidad relación de la base de datos 4 Matriz de compatibilidad 5 Código fuente de los sistemas. Verificar que las bitácoras de registro del sistema y de la infraestructura tengan todo lo necesario para conocer los posibles incidentes.	